COMBATING TERRORISM TECHNICAL SUPPORT OFFICE

2016 REVIEW BOOK

CTTSO is committed to providing technical solutions to fill the capability gaps of our operators serving in front lines overseas and of our law enforcement and first responders here at home. Our nation has made tremendous strides to prepare for and defend against terrorist attacks and other challenges to our national security; however, it is likely that these threats will be with us for decades to come. Although the United States and its Allies have made progress in Iraq and Syria against ISIL, ISIL continues to expand its influence into other theaters.

Terrorists have been largely associated with physical acts of extreme violence, but their exploitation of the information environment and social media to shape and manage their narrative underscores the need for the United States to ensure operators are properly skilled and equipped to work in the digital domain. And while we must be better prepared to operate in the new digital environment, we will continue to address the more conventional threats, such as use of tunnels, small unmanned aircraft systems, and improvised explosive devices. Additionally, we will strive to improve, lighten, and make more effective the lethal weapons and communications systems our troops need to operate effectively in the field.

This review book highlights some of our successes in 2016 and forward-looking technologies that will support the United States' posture in combating terrorism.

COMBATING TERRORISM TECHNICAL SUPPORT OFFICE

MISSION

The mission of the Combating Terrorism Technical Support Office (CTTSO) is to identify and develop capabilities to combat terrorism and irregular adversaries and to deliver these capabilities to Department of Defense (DoD) components and interagency partners through rapid research and development, advanced studies and technical innovation, and provision of support to U.S. military operations.

History and Organization

The Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict (ASD SO/LIC) established CTTSO in 1999 to consolidate its research and development programs previously administered by the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). The research and development effort that supports the interagency, Technical Support Working Group (TSWG), was the first program to transition to CTTSO.

The Explosive Ordnance Disposal/Low-Intensity Conflict (EOD/LIC) Program, which developed advanced technologies for Joint Service EOD and Special Operations Forces (SOF) missions, transitioned in 2001. In 2007, the Irregular Warfare Support (IWS) Program was initiated to satisfy a growing need to improve the capacity of the United States to counter insurgencies and fight an irregular war. In FY16, portions of the EOD/LIC and IWS Programs that support the CTTSO mission were transitioned to TSWG under the Improvised Device Defeat/ Explosives Countermeasures and Irregular Warfare and Evolving Threats Subgroups, respectively.

CTTSO and Other Agencies

CTTSO is charged with providing a forum for interagency and international users to discuss mission requirements to combat terrorism, prioritize these requirements, fund and manage solutions, and deliver capabilities. CTTSO accomplishes these objectives through rapid prototyping of novel solutions developed and field tested before the traditional acquisition systems are fully engaged. This low-risk approach encourages interdepartmental and interagency collaboration, thereby reducing duplication, eliminating capability gaps, and stretching development dollars.

CTTSO accomplishes its mission in three ways. First, CTTSO takes operational requirements from warfighters, incorporates policy priorities of the Department of Defense (DoD) civilian leadership[1], and rapidly identifies, develops, and delivers advanced capabilities for Special Operations Forces and General Purpose Forces to improve the capacity of the DoD to combat terrorism and irregular adversaries. Second, CTTSO collaborates with and supports related requirements of non-DoD U.S. government agencies and state/local/tribal governments to understand those users' priorities and requirements to share expertise, and to develop mutually beneficial capabilities. Third, CTTSO works with partner country ministries of defense under bilateral arrangements to conduct cooperative research and development, which allows the U.S. DoD to leverage foreign experience, expertise, and resources in the fight against terrorists and their infrastructure.

Technology Transition

Technology transition is the process of taking a technology from the developmental and prototype phase to production and deployment by the end user community. Transition success is achieved when research and development products have evolved to the commercial market and/or have been inserted into government acquisition programs and can be easily and continuously obtained by the combating terrorism community. The path from the research and development phase to transition success can be challenging, and it is the mission of the Technology Transition program at CTTSO to help overcome transition challenges to ensure success for the developers and end users. The Technology Transition program at CTTSO works with internal program managers, external government agencies, end users, industry, and developers to overcome any barriers that may prohibit the successful transition of CTTSO technologies.

Planning for technology transition starts at the beginning of the CTTSO business cycle and continues throughout the lifecycle of the program. In order to increase the likelihood of transition success, Technology Transition Plans are developed to provide a framework for how the technology will transition to the commercial market and/or government acquisition. Topics discussed in the Technology Transition Plan include:

- The capability gap addressed by the development of the technology;
- Identifying customers and defining the market size;
- Understanding and managing intellectual property and data rights;
- Production strategies, including partnering, investment capital, and licensing;
- Commercialization and affordability;
- Environment, safety, and regulatory issues;
- Security and export control provisions;
- Test and evaluation planning and independent operational testing; and
- Operational suitability and operational support planning.

The keys to accelerating the complicated process of moving many prototypes to production includes having a disciplined process, available assistance, and teamwork among the project manager, technology transition managers, and developers. Additional information is available at the Technology Transition section of the CTTSO website, http://www.cttso.gov.

Innovation

In the current budget environment of focusing on doing more with less, the need for innovation increases as we look for new ways to combat terrorism. Novel solutions come from individual entrepreneurs and tinkerers, and in order to leverage those solutions, CTTSO must constantly look for ways to actively engage them. The Innovation program at CTTSO has, at its core, the following objectives:

- Identify new ways to obtain success, rather than uncertain development, through prizes, challenges, and other rewards;
- Provide additional tools and resources to fulfill operational capability gaps;
- Increase the number and diversity of solution providers;
- Provide rapid and agile ways of doing business that lower both cost and risk.

[1]*Applicable policy guidance includes Presidential National Security Strategy, Defense Strategic Guidance, and any guidance or instructions issued by the ASD SO/LIC.*

Innovation is a model that enables Government research and development programs to identify the best solutions in the shortest amount of time possible at a lower cost. The following initiatives are underway at CTTSO to support the Innovation program.

- Rapid Innovation Fund: Facilitates the rapid insertion of innovative small business technologies into government systems or programs that meet critical national security needs.
- Challenge Driven Innovation: Crowdsourcing challenging problems to the world to provide ideas and solutions to fulfill important scientific and technical challenges.
- In-Q-Tel: Not-for-profit strategic investor who identifies, adapts, and delivers innovative commercial technology solutions to support the missions of the U.S. government.
- Laboratory Innovation Crowdsourcing (LINC): Conduit for field operators to submit their operational challenges to solvers in the U.S. Government.

International Partners

International cooperation allows CTTSO to leverage foreign experience, expertise, resources, and infrastructure in a unified approach against terrorism for the benefit of all. Therefore, in addition to its domestic interagency efforts, CTTSO directly manages bilateral agreements with five partner countries: Australia, Canada, Israel, Singapore, and the United Kingdom.

We have decades long histories of mutual support, technical cooperation, and information sharing. The rise of international terrorism began hundreds of years ago but reached new depths in the 1960s and 70s. Its subsequent proliferation in the 21st century spurred U.S. efforts to broaden the scope of cooperative activities to combat this threat to international peace and security.

From modest beginnings in the early 1990s, CTTSO's international relationships have matured and grown into wide-ranging and multifaceted programs that address a variety of technically sophisticated threat capabilities employed by terrorist groups and their state sponsors. Tactics, techniques, procedures, countermeasures, and associated equipment identified, developed, and tested under terms our expanding cooperative arrangements found their way into the inventories of U.S. and partner operators where they enhanced our respective national capabilities and permitted all partner nations to respond more effectively to the threats.

The partnerships provide insights into regional affairs, access to a broader technology base, and allows for the use of unique facilities offered by each country. Each of the agreements are 50/50 cost shared, comprised of financial and non-financial contributions, to address joint requirements, reducing duplication of efforts and scientific trial and error. Bilateral meetings are held on a regular basis to review ongoing projects and to discuss new areas of collaboration.

In addition to CTTSO's bilateral partners, CTTSO cooperates with other countries when appropriate. Dozens of operational capabilities developed with CTTSO partners are currently in service with a variety of personnel both throughout the United States and around the world.

Our international partnerships continue today and will for the foreseeable future as we strive to blunt the efforts of those who would seek to destroy our freedoms and compromise our way of life.

TECHNICAL SUPPORT WORKING GROUP

MISSION

The mission of the Technical Support Working Group (TSWG) is to identify, prioritize, and coordinate interagency and international research and development (R&D) requirements for combating terrorism. Through the Department of Defense's Combating Terrorism Technical Support Office and funding provided by other agencies, the TSWG rapidly develops technologies and equipment to meet the high-priority needs of the combating terrorism community, and addresses joint international operational requirements through cooperative R&D with major allies.

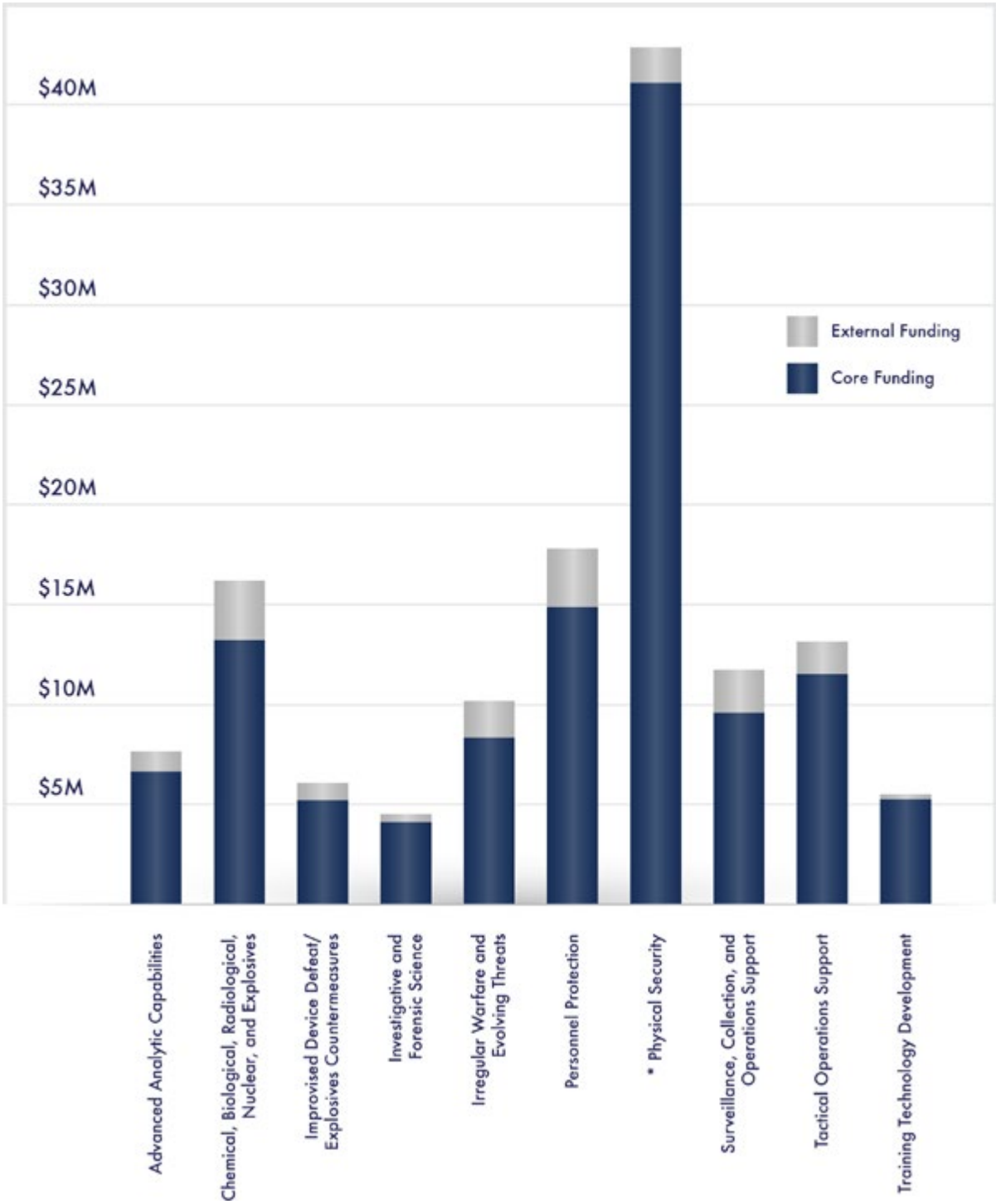
History and Organization

In April 1982, the National Security Decision Directive 30 assigned responsibility for the development of an overall United States policy on terrorism to the Interdepartmental Group on Terrorism (IG/T), chaired by the Department of State. TSWG was an original subgroup of the IG/T, which later became the Interagency Working Group on Counterterrorism (IWG/CT). In its February 1986 report, a Cabinet-level Task Force on Counterterrorism, led by then Vice President Bush, cited TSWG as assuring, "the development of appropriate counterterrorism technological efforts."

TSWG operates under the management and technical oversight of the Department of Defense (DoD) Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict (ASD SO/LIC) and the policy oversight of the Department of State's Bureau of Counterterrorism and Countering Violent Extremism.

TSWG's 10 subgroups are chaired by senior representatives from DoD, other federal agencies, and national organizations with special expertise in those functional areas. Chairmanship of subgroups is as indicated in the organizational chart below.

TSWG Fiscal Year 2016 Project Funding ($137M)



* $40M congressionally directed for cooperative anti-tunnel work with the Government of Israel.

ADVANCED ANALYTIC CAPABILITIES

aacsubgroup@cttso.gov

FOCUS AREAS

Data to Decision Systems

Develop data for decision systems that integrate and deploy predictive analytic tools and models for planning and execution of operations that include the human terrain and non-kinetic effects. Enable better and faster decisions allowing for more rapid adaptation to changes in theaters of operations.

Decision, Planning, and Analytical Tools

Develop stand-alone tools, models, and enabling technologies that provide new capabilities for improved military and interagency sense making. Successful technologies may be transitioned as an independent capability and/or integrated into larger systems.

Integrated Analytic Platforms

Develop and deploy robust integrated platforms that both operators and intelligence analysts can use to synchronize operations and intelligence at the tactical level.

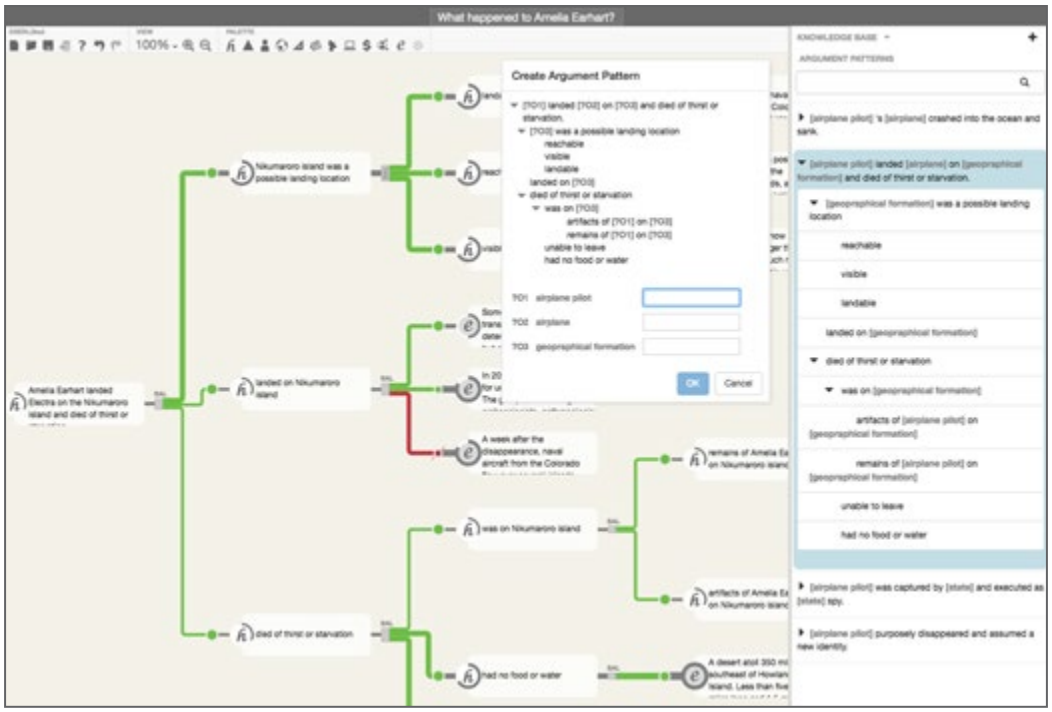
COMPLETED PROJECTS

Advanced Social Network Analysis (SNA)

Law enforcement organizations can benefit from better analytical tools when fighting organized crime in order to take down criminal networks. Criminal networks are large and complex and although there may be a wealth of data about its activities, it is problematic to analyze and make use of this information in a timely fashion. In order to address user community needs, the Naval Postgraduate School (NPS) CORE Lab, working with law enforcement communities of interest, developed a national-level, "Codebook for Law Enforcement" that provides a common ontology and set of relational definitions that will help facilitate data collection and analysis. The products of these data analyses can be used across multiple jurisdictions, making law enforcement organizations more effective in countering criminal networks. The project has transitioned to the Department of Defense, Domestic Preparedness Support Initiative (DPSI) Office for further evaluation.

Argument Mapper for Structured Reasoning

Intelligence analysts require an easy-to-use argument mapping software that creates diagrams to visually layout reasoning and evidence for and against a statement or claim. Uncharted Software, Inc. developed the Argument Mapper, a software tool that provides a structured means to organize thinking by showing the logical relationships



between thoughts that are expressed simply and precisely. As a result, analysts can identify and define patterns found in analyses, store complete work in a common knowledge base to capture analytic problem solving approaches, and apply historic methodology to new scenarios. Novice analysts can jumpstart analyses and reuse expertise, while experienced analysts can avoid recreating arguments and circumvent errors of recall or omission. The Argument Mapper is being reviewed for use by the intelligence community and is currently available to government users for a licensing fee.

Cognitive Counter-Improvised Explosive Device Signature System (C2IS2)

To more effectively address the global IED threat, a better understanding of the network of activities that surround cradle-to-grave IED use is needed. The Cognitive Counter-Improvised Explosive Device Signature System (C2IS2) software allows analysts and operators to model and analyze an adversary's network. C2IS2 includes a comprehensive browser-based user interface to enable collaboration between users and is configured to allow subject matter experts to capture detailed information that all-source and single-source analysts can use to develop better multi-source collection plans. This project is being transitioned to the Joint Improvised-Threat Defeat Organization and several other government agencies for use.

Combating Terrorism Technology Startup and Advanced Analytic Application Challenges

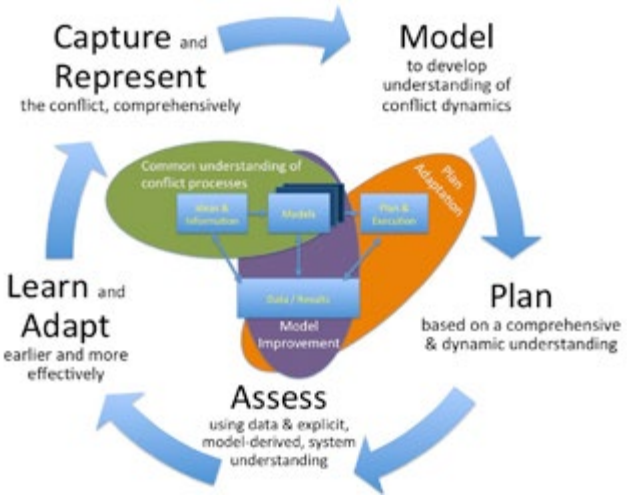
CTTSO in partnership with the Israel Ministry of Defense, Directorate of Defense Research and Development and the MIT Enterprise Forum of Israel, executed the Combating Terrorism Technology Startup and Advanced Analytic Application Challenges in Tel Aviv, Israel. The purpose of the competition was to illuminate technology innovation in Israel and identify alternative performers to traditional government vendors among startup companies, research groups, and entrepreneurs. Between both challenges, over 150 companies submitted phase one proposals, which were evaluated by a multi-disciplinary panel of experts representing United States and Israeli Governments, industry, and academia.

In addition to events related to the challenges, leading experts from the Government of Israel, academia, and industry presented on a variety of topics, from the latest terrorism trends to guidance for achieving success as a security startup. This event also included an exhibition featuring over 20 companies developing a wide variety of capabilities relevant to the national security sector.

ONGOING PROJECTS

Model Enabled Analysis, Design, and Execution (MEADE)

Decision making in support of U.S. national security and foreign policy issues is difficult due to complex socio-political challenges that arise in dealing within the human domain. Predictive modeling that can help campaign planners better understand the potential impacts of their decisions in order to not further complicate the social environment in which a campaign may take place is needed. CTTSO is working with System of Systems Analytics, Inc. to develop the Model Enabled Analysis, Design, and Execution (MEADE), a series of tools, models, and methodology that is being developed to support Military Decision-Making Planning (MDMP). MEADE, through a spiral development process, is using sample datasets in order to evaluate the model's performance with regard to predictive accuracy. Currently, a series of studies with members of the user community are being conducted in order to provide feedback that can be used to tailor MEADE outputs in order to further improve its predictive capabilities.

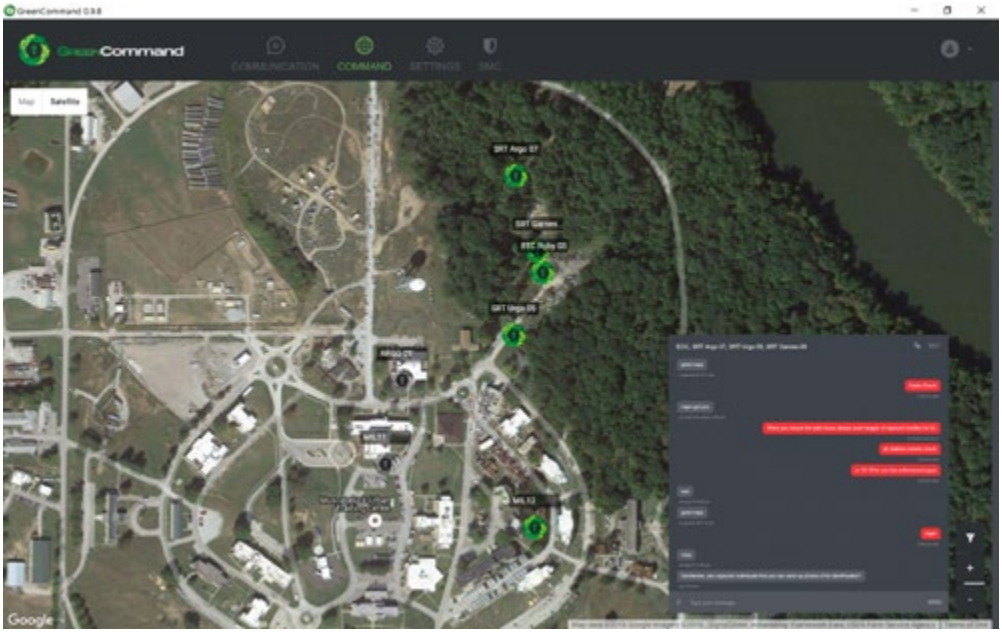


Operate to Know (OtK)

U.S. Marine Corps warfighters are frequently required to operate, with little preparation time, in environments where they are lacking key information about who the enemy is, where they are, what they are doing, and what their intentions are. Experts from System of Systems Analytics, Inc. are supporting CTTSO and the U.S. Marine Corps to develop Operate to Know (OtK), a concept of operations (CONOPS) that synchronizes unit operations with supporting intelligence and information in order to improve the timeliness and comprehensiveness of actionable intelligence. Many models, workflow engines, visualization tools, and anticipatory analytics developed through other CTTSO efforts will be applicable to CONOPS developed for this effort. In August 2016, the ability of the U.S. Marine Corps to coordinate intelligence, surveillance, and reconnaissance (ISR) data required for OtK analyses was demonstrated at China Lake as part of Enterprise Challenge –16.

Secure Information Sharing (SIS) Prototype

Law enforcement face many challenges related to cybersecurity; secure, unclassified information sharing; and tactical surveillance. The Secure Information Sharing (SIS) Prototype project provides a range of advanced, secure communications, tactical surveillance, and change detection for federal, state, and local law enforcement organizations. The SIS project will integrate secure tactical communications capabilities, intelligence automation systems, secure information sharing, advanced video surveillance, and distributed mobile computing for Android™ devices. Upon completion, SIS will be piloted with several interagency partners.



MEMBERSHIP

Intelligence Community

- Office of the Director of National Intelligence

Joint Interagency Task Force South

National Reconnaissance Office

U.S. Department of Defense

- Defense Intelligence Agency
- Joint Improvised-Threat Defeat Organization
- National Geospatial-Intelligence Agency
- Naval Postgraduate School
- Office of the Secretary of Defense (Rapid Fielding Office)
- Office of the Secretary of Defense, Homeland Defense and Americas' Security Affairs
- Office of the Secretary of Defense for Special Operations and Low-Intensity Conflict
- Special Operations Command Central
- U.S. Army G-2, G38
- U.S. Marine Corps Intelligence Department
- U.S. Special Operations Command
  - Army Special Operations Command

U.S. Department of Homeland Security

- Customs and Border Protection
  - Border Patrol
- Office of Intelligence and Analysis

U.S. Department of Justice

- Federal Bureau of Investigation

U.S. Department of State

- Bureau of Counterterrorism and Countering Violent Extremism
- Bureau of Near Eastern Affairs
- Office of Science and Technology Policy

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVES

cbrnesubgroup@cttso.gov

FOCUS AREAS

CBRNE Characterization and Attribution

Systematically investigate and identify the unique physical and chemical characteristics of CBRNE materials; develop tools to determine the origin of CBRNE agents and materials; and evaluate clandestine methods of chemical and biological agent and homemade explosives production.

Consequence Management

Develop CBRN decontamination solutions, tools, and techniques; develop decision support tools which analyze, aggregate, and integrate multi-source data to provide enhanced on-scene situational awareness and risk assessment capabilities for CBRNE response; and develop training solutions to enhance the operational effectiveness of CBRNE operators.

Protection

Develop respiratory and dermal protective equipment to minimize exposure to CBRN materials while operationally enhancing individual performance; enhance shelter-in-place capabilities; and develop materials, tools, and techniques for hydration systems in compromised environments.

Detection and Identification

Develop equipment, tools, and techniques to sample, detect, and identify trace (gases, vapors, and non-visible amounts of solid and liquid) and bulk (microgram and higher amounts of solid and liquid) amounts of CBRNE threat materials at point, proximity (inches), and standoff (meters to kilometers) distances in both fixed and on-the-move configurations.

COMPLETED PROJECTS

Handheld Mass Spectrometer

Mass spectrometry has the potential to provide high sensitivity, high selectivity, and broad detection for a wide range of threats; however, these systems typically weigh at least 35 to 40 pounds and are not robust enough for the field. 908 Devices, Inc. developed a lightweight mass spectrometer for trace detection and identification that brings sensitivity and selectivity to the field along with a new level of robustness and usability.

The system, known as the MX 908, uses a micro-ion trap array approximately the size of a U.S. 25-cent piece, reduced from the approximate size of a soda can. This reduction in size significantly shortens the path of the ions and allows the mean free path of the ions to be shorter while maintaining good resolution; therefore, the system can operate at a pressure that is orders of magnitude higher and rely on much smaller and more durable pumps. The system is less than seven pounds and while this effort focused on detection of liquid and solid trace materials being introduced off of a swab, the system also performs vapor detection in both a continuous and single sample mode. The system initializes and is operational in less than a minute and gives results in seconds with dual polarity interrogation of each sample. This system provides a handheld capability for detection of explosives, toxic industrial chemicals, chemical warfare agents, and drugs. Five systems were delivered for test and evaluation in the first quarter of FY17.

Next Generation Chemical and Biological (CB) Sock

Responders to CB incidents require personal protective equipment that provides the needed level of protection from CB hazards along with a necessary level of comfort to complete routine and emergency operations. Current CB socks are uncomfortable, not form fitting, and have excess material which tends to cause the material to bunch in the toe or heel region.

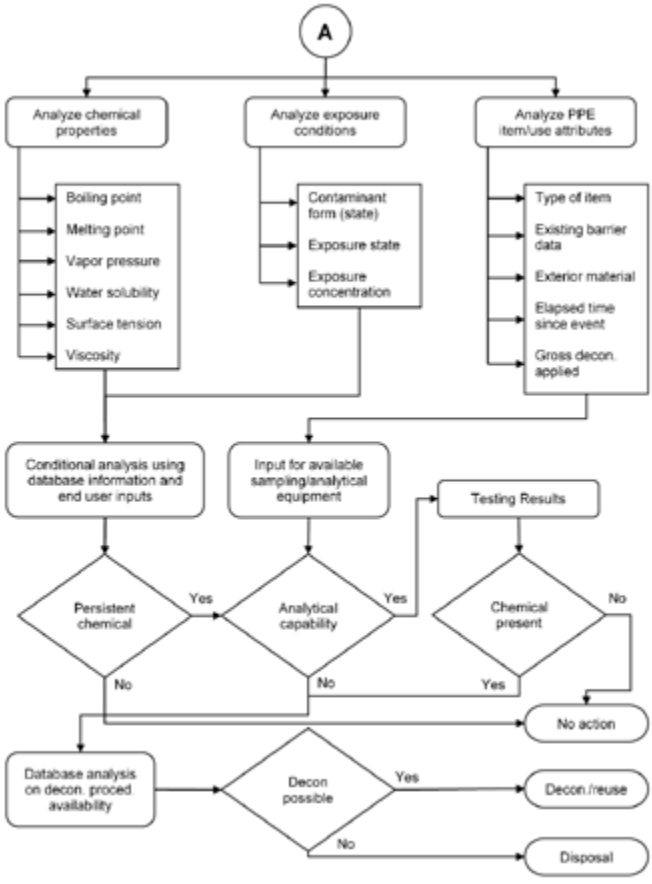
North Carolina State University Textile Protection and Comfort Center, in partnership with Lion Apparel, Inc. and W. L. Gore & Associates, Inc., developed the next generation CB protective sock that provides National Fire Protection Association (NFPA) 1994, Standard on Protective Ensembles

for First Responders to Chemical, Biological, Radiological, and Nuclear Terrorism Incidents, Class 3 protection when worn under CB boots or tactical footwear. The next generation CB sock provides extended mission percutaneous protection from exposure to the harmful effects of all traditional CB warfare agents and the toxic industrial chemicals listed in NFPA 1994 Class 3. The CB sock is made from a stretch material in a form fitting design that provides exceptional mobility and comfort. The CB sock can be worn in temperature and humidity extremes while withstanding salt spray, seawater, rain, sand, dust, sweat, oil, and other contaminants. Its sleek, lightweight, breathable design easily integrates with a variety of protective ensembles and can be laundered for multiple cycles.

Non-Destructive Chemical and Biological Analysis Techniques Enabling Effective Personal Protective Equipment Decontamination Strategies

International Personnel Protection, Inc. developed a comprehensive document to provide first responder organizations with information on specific techniques to non-destructively evaluate their personal protective equipment (PPE) for chemical and biological contaminants. The project was aimed at reusable PPE that includes relatively expensive items such as garments, footwear, and gloves, and will allow first responder organizations to decide if PPE can be safely decontaminated and reused.

The report determined that the most accurate means to non-destructively assess contamination levels of reusable PPE involve wipe sampling and head space collection coupled with laboratory-based analyses. The guidance highlighted the differences between sampling approaches and the ability to apply non-destructive analysis. Project findings were transitioned by making specific recommendations to industry standards for addressing contamination assessment and decontamination of PPE.

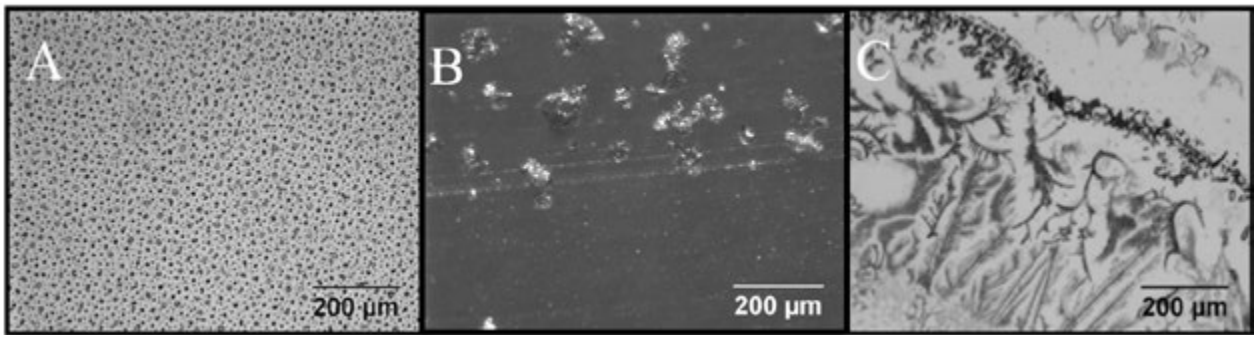


Small Unit Water Purifier (SUWP)

Existing bulk water treatment systems are too large, power intensive, and require specially trained operators. By contrast, individual water purifiers (IWPs) produce enough water to supply the individual warfighter for several weeks but are not designed for extended use. A treatment system between individual and bulk use, termed a Small Unit Water Purifier (SUWP), was a significant gap within the U.S. Department of Defense. The water treatment system developed under this project reduces the resupply of bottled water and fielded individual water purifiers.

The SUWP, developed by Cascade Designs, Inc., removes suspended solids, colloidal matter, dissolved organic and inorganic chemical contaminants, and microbiological pathogens to create potable water that passes NSF P248 and meets the TBMED-577 standard for potable water. The total weight of the pelican case containing all components weighs 105 pounds and the core of the system (a self-sustaining backpack) weighs only 28 pounds. Included in the pelican case are both an electrical pump box and a manual foot pump, either of which can operate the system in order to give users a man-powered option. A small amount of disinfectant residual is automatically added to the filtered water to prevent recontamination during storage. The average flow rate of the system is four liters per minute which allows users to produce enough water to stay healthy and maintain optimal performance.

Development of Standoff, Explosive Detection, Standard Test Materials



A) Aerosol Spray Deposition *B) Ink-Jet Deposition* *C) Direct Deposition*

Image courtesy of the Transportation Security Laboratory

Detection systems being developed allow operators to detect trace explosive and identify a threat without getting near it. Assessing and evaluating these state-of-the-art systems are a challenge because the test methodology must be relevant to real-world situations and use test samples of trace explosive depositions with known distributions and total amounts that are highly consistent from sample to sample.

This effort refined various techniques used to prepare standard test materials of deposited explosives in the form of fingerprints. Multiple U.S. Government and international laboratories to include the Department of Homeland Security-Science and Technology Directorate's Transportation Security Laboratory, Army Research Laboratory, Edgewood Chemical and Biological Center RDECOM, National Institute of Standards, and the United Kingdom's Defence Science and Technology Laboratory, compared methodologies for a wide range of threats, particle sizes, and distributions that replicate realistic trace fingerprints.

Samples from each technique were characterized optically and analytically to develop a consensus sample that is stable, accurate, reliable, and realistic. These standards will be used to evaluate non-contact and/or standoff explosives detection technologies in a way that provides meaningful and relevant results to the scientific community and users. Standard preparation methods have been shared across participating organizations for use in future government testing.

ONGOING PROJECTS

Carbon Monoxide and CBRN Low Profile Escape Respirator

In the event of an accidental or terrorist chemical release where there is also smoke nearby, people need immediate access to respiratory protection against both the threat and the carbon monoxide in the smoke. Traditionally, air-purifying escape respirators which protect against carbon monoxide and chemical, biological, radiological, and nuclear (CBRN) inhalation hazards are large and cumbersome, which in some cases makes them impractical to have on hand at all times.

Avon Protection Systems, Inc. is developing a pocket-sized escape respirator to provide protection from carbon monoxide and CBRN inhalation hazards. The new escape respirator leverages the latest carbon monoxide absorbent catalyst technology and will meet the requirements of the National Institute for Occupational Safety and Health Statement of Standard for Chemical, Biological, Radiological, and Nuclear – Air Purifying Escape Respirator. The ultra-slim, low-profile escape respirator is intended for use by the general adult working population. The lightweight respirator will be small enough to discreetly carry or store in a pocket, constructed of flame and heat resistant materials, require no annual fit testing or maintenance, and have a minimum duration of 15 minutes.

First Responder Biological Personal Protective Equipment

Responding to biological hazards poses unique challenges for garments that must protect users while allowing them to effectively perform their duties. Unlike chemical incidents, biological incidents are typically not confined to the location of the release and users are required to work for long periods of time in areas where people may be infected. Biological threats require a specific approach to doffing that is not addressed in other protective clothing.

International Personnel Protection, Inc. teamed with Blauer Manufacturing Company, W. L. Gore & Associates, Inc., ILC Dover, Cornell University, and Intertek Testing Services to develop multiple-use biological personal protective equipment that provides National Fire Protection Association (NFPA) 1999, Standard on Protective Clothing for Emergency Medical Operations, and National Fire Protection Association (NFPA) 1994, Standard on Protective Ensembles for First Responders to CBRN Terrorism Incidents, Class 4 protection. Two specific ensemble designs being developed provide a range of potential clothing solutions for biological and radiological particulate protection. They will be low cost, lightweight, multi-functional first responder ensembles that address multiple clothing item integration, provide reasonable levels of durability and improved breathability for long-term wearing comfort, and permit easy doffing and removal.

HazMat Suit Communications System

Responders to chemical/biological incidents can range from military personnel and fire fighters to law enforcement and homeland security. Each specific group has personal protective equipment (PPE) specially designed for their individual needs but lacks an effective communications system. Current head-worn PPE muffles speech and impairs hearing, thereby limiting effective use of external communications equipment (headsets, speaker microphones, and/or radios). Wearing a system internally to PPE may compromise sealing of the PPE and present a risk of exposure.

Gentex Corporation is developing a communications system that works with Class 2 and Class 3 garments that are National Fire Protection Association 1994, Standard on Protective Ensembles for First Responders to CBRN Terrorism Incidents compliant, without compromising any interfaces or closures. The system consists of four major components, the headset with throat microphone and two earplugs, inner module, outer module with optional boom microphone connection, and push-to-talk. The battery operated system provides low power, short range infrared connectivity between the inner and outer modules. The communications system is suit and mask agnostic allowing integration with a variety of Class 2 and Class 3 protective garments and respirators. The new communication system assures seal integrity and does not require any garment or respirator modifications.

Collection Infrastructure for Wireless Information from Detectors

The safety of firefighters, police officers, and other emergency responders at chemical, biological, radiological, nuclear, and explosives (CBRNE) incidents is essential to the effective resolution of the incident. The selection and application of risk control measures to minimize and prevent exposures are dependent on the information responders have about the incident and the characterization of the environment. Unfortunately, many of the tools that are provided to first responders are unable to communicate with each other or with the emergency response command structure.

Collection Infrastructure for Wireless Information from Detectors (CIWID) retrieves real-time information from various handheld CBRNE sensors and wirelessly transmits the data back to a central location to assist in the on-scene management of exposures. The project developed complementary electronics to demonstrate the utility of the First Responder Sensor Protocol, a common communication method for CBRNE sensors which does not rely on proprietary solutions. The CIWID interfaces directly with CBRNE sensors via a CIWID "dongle" – a small, rugged enclosure of a printed circuit board that communicates wirelessly with each other and a central gateway. This gateway presents the sensor data and the dongle's location to authenticated consumers via a web interface

Currently, Kopis Mobile, LLC has developed hardware solutions for serial port (RS232), infrared, and Bluetooth sensor interface types. Future plans exist for transistor-transistor logic (TTL), Ethernet, isolated general purpose input output interface (Isolated GPIO), and Universal Serial Bus (USB) sensor interface types.

Double Blind Assessment of Non-Contact and/or Standoff Explosives Detection Technologies

As state-of-the-art non-contact and standoff detection systems continue to be developed, users are left with the challenge of validating system performance and reliably evaluating systems against the real life situations they face. A worldwide request for information was issued to identify state-of-the-art, commercial-off-the-shelf and government-off-the-shelf advanced-stage prototypes and technologies for the trace or near-trace detection of contraband materials (explosives, narcotics, and other chemicals) at standoff or non-contact distances in order to evaluate these systems in a consistent and realistic way.

The "Double Blind Assessment of Non-Contact and/or Standoff Explosives Detection Technologies" uses standard test materials developed under the "Standard Test Materials for Chemical/Explosive Contamination" project to assess systems from a wide range of technology readiness levels, with standoff capabilities ranging 30 centimeters to greater than 4 meters. The volunteer-based assessment evaluates state-of-the-art technologies ranging from multiple categories of quantum cascade lasers (QCL), various Raman technologies such as coherent anti-Stokes Raman spectroscopy (CARS), and infrared and laser-induced fluorescence. The assessment evaluates the detection capabilities on eleven potential threats at various loads using three different deposition methods. The systems will be challenged with double blind test articles which mimic automobile surfaces with the goal of assessing capabilities at realistic levels of trace explosives in a simulated environment in order to determine the technology readiness of standoff detection systems for the user community. This work is in collaboration with the Department of Homeland Security-Science and Technology Directorate's Transportation Security Laboratory and is being performed by Signature Science, LLC.

Ruggedized National Fire Protection Association (NFPA) 1994 Class 2 Ensemble

Responders to chemical incidents range from military personnel and firefighters to law enforcement and event security personnel. Each group has protective equipment specifically designed for their individual needs while providing the needed level of protection from chemical, biological, and radiological hazards. Current ensembles have known issues with proper fit, security of head protection, maintaining an adequate seal with the respirator mask, lack of comfort, and restricted mobility.

North Carolina State University Textile Protection and Comfort Center, in partnership with Lion Apparel, Inc. and W. L. Gore & Associates, Inc., is developing an enhanced next generation Class 2 multi-threat ensemble that will be NFPA 1994, Class 2 protection compliant. The new ruggedized Class 2 ensemble will be a lighter, one-piece garment that has better interoperability with protective and mission-oriented equipment in order to provide full body protection. The ensemble will be optimized for interoperability with helmets, body armor, communications equipment, ammunition loads, and personal weapons.

Ruggedized National Fire Protection Association (NFPA) 1994 Class 3 Ensemble

Blauer Manufacturing Company, in partnership with International Personnel Protection, Inc., W. L. Gore & Associates, Inc., Avon Protection Systems, Inc., and AirBoss Defense, is developing the next generation NFPA 1994 ruggedized Class 3 compliant ensemble for chemical, biological, and radiological protection of first responders. The ruggedized Class 3 ensemble is intended to expand the ability to accommodate different types of mission equipment among first responders, and specifically, provide improved durability and overall protection.

The project team has focused on improving the fit and functionality of Blauer Manufacturing Company's existing NFPA 1994 Class 3 suit, especially in the area of equipment integration. The product uses a new ruggedized W. L. Gore material that is more durable, provides a greater level of cut and puncture resistance, as well as an equally breathable material with extended permeation resistance. Specific attention was paid to the hood and torso areas for improved use with ballistic helmets and vests, along with the use of reinforcing fabrics at critical contact areas of the ensemble. The ensemble will be certified to NFPA 1994, Class 3 in addition to NFPA 1992.

Scalable Vacuum Evidentiary Powder Collection Device

The 2001 anthrax letter attacks demonstrated both the extreme hazard of collecting and handling biological agent powders and the importance of recovering as much of the agent as possible for forensic analysis. Response personnel use standardized methodologies for collecting suspicious powders. The frequency of suspicious powder incidents requires a complementary methodology that will provide response personnel with a device capable of rapidly and efficiently collecting powders while minimizing the generation of hazardous aerosols.

Seacoast Science, Inc. is developing a portable and scalable evidence collection device capable of collecting and isolating powders by vacuum into a sterile, sealable laboratory vial. The collection device will have a disposable front section that can be separated, capped, and placed in an evidence bag after sample collection, preventing sample loss and cross-contamination. The prototype collection device is on track for delivery in 2017.

Personal Chemical Sensor (Black Canary)

Many toxic chemical vapors are invisible, may be odorless, and are dangerous even at extremely low concentrations. Exposure to toxic chemicals through nefarious means or accidents can cause grave harm to military personnel, first responders, law enforcement, and civilians. This project will lead to the development of a new wearable sensor designed to issue early warning to the presence of toxic chemical vapors, thereby allowing the responder to adopt the appropriate risk control measures.

The sensor system, dubbed Black Canary, was developed by Ideation Product Solutions through collaboration with Australia's Defence Science and Technology Group and is based on color change chemistry paired with a cutting edge opto-electronics design. Thumbnail-sized, swappable cartridges, specifically targeted for toxic vapors of interest, plug into receptors on a mobile phone-sized device. Each cartridge is a miniaturized, single wavelength spectrometer comprising of a reactive chemical sample, casing, and electronics package. When plugged into the device, the temperature and humidity stabilized cartridges are automatically recognized for the chemical of interest and self calibrated. The device draws air past the reagents located on each cartridge and handles data processing and pattern recognition automatically, allowing the user to operate unhindered until an alarm is triggered.

Black Canary meets an identified gap in the toxic vapor detection space, offering the simplicity of operation with a level of sophistication usually associated with larger handheld devices. The capability will be affordable, easy to operate, and adaptable to meet end user needs. Currently, eight cartridge types (hydrogen cyanide, hydrogen sulfide, sulfur dioxide, chlorine, phosphine, nitrogen oxides, ammonia, and hydrogen chloride) have been developed that detect at, or below, the United States Occupational Safety and Health Administration defined Permissible Exposure Limits.

MEMBERSHIP

Environmental Protection Agency

Federal Reserve Board

Intelligence Community

InterAgency Board

State and Local Agencies

- Alexandria (VA) Fire Department
- Arlington County (VA) Fire Department
- Boston (MA) Fire Department
- City of Orlando (FL) Police Department
- District of Columbia Fire Department
- District of Columbia Metropolitan Police Department
- Douglas County (GA) Emergency Management Agency
- Douglas County Fire Department
- Douglas County Sheriff's Office
- Fairfax City (VA) Fire Department
- Fairfax County (VA) Fire and Rescue Department
- Fairfax County Police Department
- Los Angeles (CA) Police Department
- Metropolitan Nashville (TN) Police Department
- Nashville Fire Department
- New York City Fire Department
- New York City Office of Chief Medical Examiner
- New York City Police Department
- Northern Illinois Police Alarm System
- Raleigh (NC) Fire Department
- Seattle (WA) Fire Department
- Virginia Department of Emergency Management
- Virginia Department of Transportation

U.S. Capitol Police

U.S. Department of Agriculture

- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service

U.S. Department of Commerce

- National Institute of Standards and Technology

U.S. Department of Defense

- Acquisition, Technology, and Logistics
- Defense Advanced Research Projects Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- Joint Improvised-Threat Defeat Organization
- Joint Program Executive Office for Chemical and Biological Defense
- Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense
- Pentagon Force Protection Agency
- U.S. Air Force Air Combat Command
- U.S. Army
  - 20th Support Command, CBRNE
  - 22nd Chemical Battalion
  - Armament Research, Development, and Engineering Center
  - Chemical, Biological, Radiological, and Nuclear School
  - Medical Department
  - National Ground Intelligence Center
  - Research, Development, and Engineering Command, Edgewood Chemical Biological Center
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
  - Explosive Ordnance Disposal
  - Systems Command
- U.S. Navy
  - Bureau of Medicine
  - Naval Air Warfare Center
  - Naval Explosive Ordnance Disposal Technology Division
  - Naval Forces Central Command
  - Naval Research Laboratory
  - Naval Surface Warfare Center
- U.S. Special Operations Command

U.S. Department of Energy

- National Nuclear Security Administration

U.S. Department of Health and Human Services

- Centers for Disease Control and Prevention
- Food and Drug Administration
- National Institute for Occupational Safety and Health

U.S. Department of Homeland Security

- Federal Emergency Management Agency
- National Protection and Programs Directorate
  - Federal Protective Service
- Office of Health Affairs
- Science and Technology Directorate
  - Transportation Security Laboratory
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of the Interior

- National Park Service, United States Park Police

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Bureau of Investigation
- National Institute of Justice
- U.S. Marshals Service

U.S. Department of Labor

U.S. Department of State

- Bureau of Arms Control, Verification and Compliance
- Bureau of Counterterrorism and Countering Violent Extremism
- Bureau of Diplomatic Security
- Bureau of Overseas Buildings Operations

U.S. Department of Transportation

- Research and Innovative Technology Administration (Volpe Center)

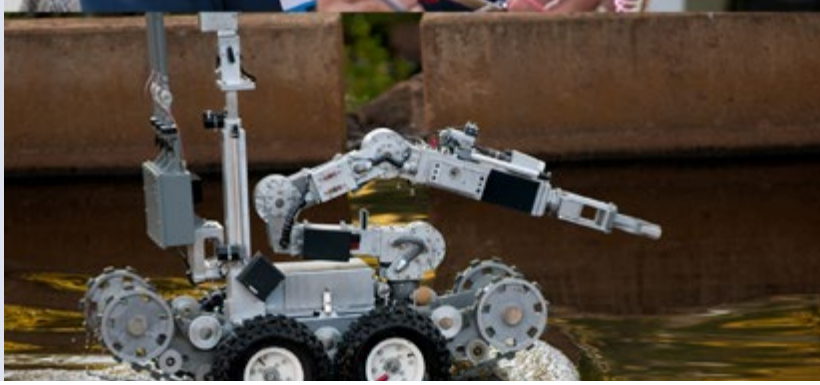
U.S. Senate Sergeant at Arms

White House

- Homeland Security Council
- Office of Science and Technology Policy

IMPROVISED DEVICE DEFEAT/ EXPLOSIVES COUNTERMEASURES

iddsubgroup@cttso.gov



FOCUS AREAS

Improvised Device Defeat

Improve or develop operational capabilities to neutralize, render-safe, and contain blast and fragmentation during improvised terrorist device, and explosives response operations.

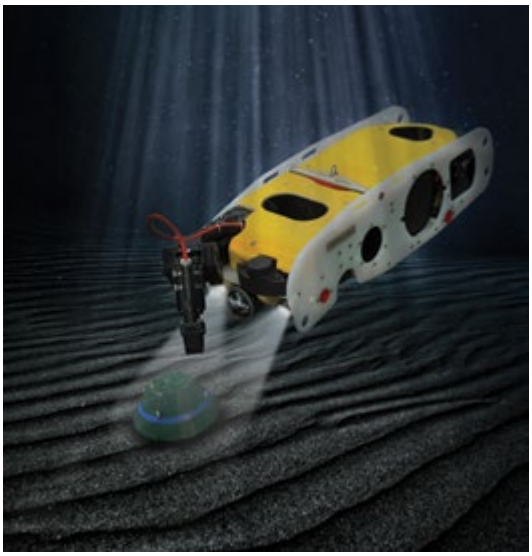
Device Diagnostics and Threat Characterization

Provide advanced technologies and technical solutions that improve identification, analysis, and technical characterization of explosives, improvised explosive devices (IEDs) and their components, and potential weapons of mass destruction in support of response operations.

Robotics and Remote Means

Develop or enhance platforms, systems, and technologies to remotely conduct activities related to the neutralization or rendering safe of IEDs, unexploded ordnance (UXO), homemade/improvised explosives and their precursors, and enhanced hazard devices containing chemical, biological, or radiological materials.

COMPLETED PROJECTS



Sea Wasp

The Sea Waterborne Anti-IED Security Platform (Sea Wasp) is a first of its kind tethered, remotely operated vehicle (ROV) designed for surveillance, location, identification, and neutralization of underwater IEDs or ordnance specifically in the confined areas and challenging environmental conditions of ports and harbors. Features include: two-man portable, six degrees of freedom mobility and versatility, way-point navigation, operates in 2.5-knot current, station keeping capabilities, and a five-function electric manipulator arm for interrogation. Three prototype systems were delivered from January through March 2016 to U.S. Navy Explosive Ordnance Disposal (EOD) Group TWO, an FBI counter-IED unit, and South Carolina Law Enforcement Division's Counter-Terrorist Operations Maritime Response Unit. All users received initial training and have conducted further testing and evaluation. Sea Wasp also participated in the Coastal Trident 2016 Regional Port and Maritime Security Program Exercise designed to advance the state of the art in addressing potential threats to the U.S. Marine Transportation System.

Vehicle-Borne Improvised Explosive Device (VBIED) Countermeasures Guide

The VBIED Countermeasures Guide was developed to provide an electronic decision support tool to assist in the full range of challenges involved in VBIED response operations by EOD Units or Public Safety Bomb Squads. The guide provides the following capabilities: situation analysis; logic flow; tool prioritization (to include probability of success); tool capability (full range of metrics from what we know, to what we do not know); tool construction for do-it-yourself tools; and tool deployment strategies. The guide ensures the safest procedure is used with the highest probability of success with the least possible collateral impact. The guide is available in a software package or application suitable for use with laptops and tablet computers and is compatible with Android, Apple, and Windows-based operating systems.

Eastern National Robot Rodeo and Capability Exercise

It is often difficult for end users to identify and articulate technology gaps. By hosting events such as the Eastern National Robot Rodeo (ENRR), the Improvised Device Defeat/Explosives Countermeasures Subgroup is able to see firsthand where improvements need to be made in robotics capabilities. During the inaugural ENRR, experienced Explosive Ordnance Disposal (EOD) and Public Safety Bomb Squads (PSBS) employed their skills in operating robots in challenging, real-world scenarios, while observers and controllers gathered information about tactics, techniques, and procedures, and technology shortfalls. The IDD/EC Subgroup partnered with the Air Force Civil Engineer Center and the United Kingdom's Defence Science and Technology Laboratory to sponsor the ENNR and

CAPEX. The event took place from August 29 to September 2, 2016 at Dobbins Reserve Air Force Base, Georgia and was co-hosted by the Transportation Security Administration from the Atlanta Hartsfield-Jackson International Airport. The event leveraged the support of Sandia and Los Alamos National Laboratories who have nine years of experience hosting the Western National Robot Rodeo and CAPEX. Participants included five EOD units, four PSBS, and the National Institute of Standards and Technology. The ENRR/CAPEX offered a prime opportunity for expert bomb squad operators and public safety professionals from around the world to gather, employ, and share advanced skills operating new robotic technologies in challenging, real-world scenarios.

ONGOING PROJECTS

Robotic Backscatter X-ray Inspection System for EOD

American Science and Engineering, Inc. (AS&E) has designed and developed a robot-mounted backscatter X-ray (Bx) system for use by Explosive Ordnance Disposal (EOD) Units and Public Safety Bomb Squads to capture single-sided images of suspected improvised explosive devices (IEDs). Unlike conventional transmission X-ray technology, Bx imaging technology highlights organic materials such as explosives and chemical-biological threats and enables single-sided imaging for added flexibility. AS&E designed the Bx imaging system for rapid mounting and deployment in the field and for remote operation and rapid interrogation of suspect objects. The system will be compatible with various robotic platforms and will mount in different configurations and onto the manipulator arm of the robot. Other key components of the system such as power, electronics, and imager stowage rest are designed to easily integrate with robot.

Worldwide IED Trend Analysis

Many times analyses and reports regarding IED incidents fail to provide IED defeat personnel with technical information that is necessary to inform development of render safe procedures if similar devices are encountered. Intelligence Management Support Services Limited is closing this information gap by collecting and collating worldwide IED technical data from 2005 to present on significant emplacement strategies, electronic circuitry, triggering mechanisms, explosive fillers, and container design for eventual inclusion in the Bomb Technician Wiki. Collected technical data includes relevant information for bomb technicians, such as information that affect diagnostics, access, and IED defeat. Delivery of information through the Wiki is organized and allows quick cross-referencing by regions of the world, country, device sophistication, device category, and component-level items.

MEMBERSHIP

Intelligence Community

International Association of Bomb Technicians and Investigators (IABTI)

Joint Program Office for Countering Improvised Explosives Devices

National Bomb Squad Commanders Advisory Board

State and Local Law Enforcement

- Arizona Department of Public Safety (Western Region)
- Delaware State Police (Eastern Region)
- Fairfax County (VA) Police Department
- Houston (TX) Police Department (Central Region)
- Maryland State Police
- Michigan State Police
- Pittsburgh (PA) Bureau of Police
- South Carolina Law Enforcement Division (Southern Region)

U.S. Capitol Police

U.S. Department of Defense

- Pentagon Force Protection Agency Bomb Squad
- U.S. Air Force
  - Air Combat Command
  - Explosive Ordnance Disposal Technical Detachment (AFCEC/CXE)
- U.S. Army
  - 52nd Ordnance Group
  - Explosive Ordnance Disposal Technical Detachment
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
  - Explosive Ordnance Disposal Detachment
- U.S. Navy
  - Explosive Ordnance Disposal Fleet Liaison Office
  - Explosive Ordnance Disposal Technology Division
  - National C-IED Knowledge Network
  - Training and Evaluation Unit ONE
  - Training and Evaluation Unit TWO

U.S. Department of Homeland Security

- National Protection and Programs Directorate
  - Office for Bombing Prevention
- Science and Technology Directorate
  - Homeland Security Advanced Research Projects Agency
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Bureau of Investigation
- National Institute of Justice

INVESTIGATIVE AND FORENSIC SCIENCE

ifssubgroup@cttso.gov

FOCUS AREAS

Credibility Assessment (Detection of Deception and Intent)

Develop improved interviewing and interrogation equipment, methods, and techniques through behavioral/operational psychology advancements, including psycholinguistics, cognitive methods, and motivational techniques.

Crime Scene Response

Improve the quality of recognition, collection, documentation, analysis, and preservation of evidence and actionable information from incident scenes for future prosecution and targeting. Create standardized field tests, collection sets, kits, and other crime scene equipment. Develop capabilities to rapidly and visually document a scene in any environment. Increase the safety and security of law enforcement first responders at a terrorism scene.

Criminalistics

Create advanced capabilities in the traditional forensic science disciplines to identify individuals and improve the recovery, identification, evaluation, and analysis of material and traces. Develop benchtop and handheld instrumentation that decreases throughput time and automates interpretation.

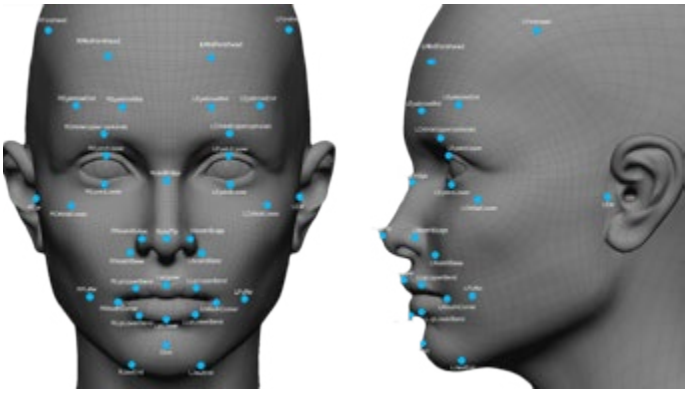
Digital and Multimedia Forensics

Develop computer forensic hardware, software, decryption tools, and digital methods to investigate terrorism. Develop advanced methods to extract, decrypt, analyze, and enhance audio recordings, video images, and other forensic information from analog and digital sources.

Forensic Exploitation

Develop a lexicon, common operating procedures, and advanced techniques for material and personnel exploitation of sensitive sites, caches, targeted objectives, and incident scenes. Advance the portable and packable expeditionary and "reach back" exploitation analysis capabilities for level I, II, and III forensic analysis. Improve law enforcement-related technical surveillance methods.

COMPLETED PROJECTS



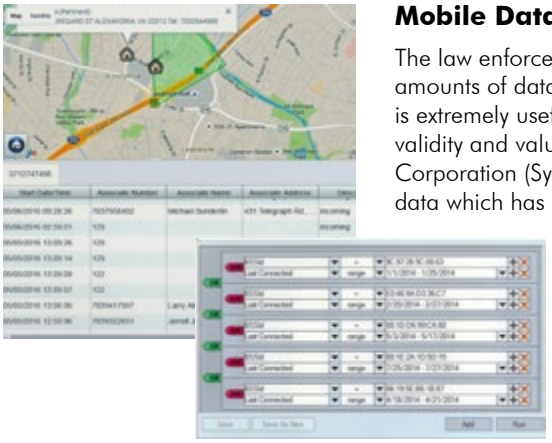
Facial Recognition/Identification from Uncontrolled Images and Video

Law enforcement and military forces often acquire videos, images, and photos which could potentially yield valuable evidence and intelligence about the persons in them. Identifying or recognizing persons in multiple forms of media is key to exploiting this actionable intelligence to deny their anonymity. One of the biggest challenges is that most of the technology only works with certain file types or has other limitations restricting its ability to provide operators with the required analysis. The facial recognition/identification from uncontrolled images and video system provides law enforcement and military forces critical evidence and intelligence from videos, images, and photos. Progeny Systems Corporation of Manassas, Virginia, developed a software application that automatically scans large volumes of digital videos, images, and photos to detect faces and heads from a range of angles. The application analyzes image or video files whose format or content is not controlled by the acquiring agency. The tool provides clustering and grouping of similar faces, as well as facial recognition of image and video data. Operators can manually edit and correct the groupings and clustering, if desired. The software can cross-match these clusters with other clustered datasets and serve as the gallery against which 1-to-N type searches may be conducted. The analysis incorporates methods and technology combining general and specific facial characteristics, unusual details such as scars and tattoos, and features about the surroundings in the images and videos to identify criminals and victims. The analysis algorithms also include computer learning techniques, biometric facial recognition enhancements, and other improved and advanced recognition technology.

Remote Image Card Unit

At checkpoints and access control points, officials may have a significant challenge when determining if an identification card is genuine or counterfeit. Many different types of identification may be presented, such as, a driver's license from any of the 50 states or a passport from over 100 countries. Officials cannot be familiar with all of these types of identification so sometimes they are unable to determine which are valid. ID Scientific of Park City, Utah, has developed the remote image card unit which solves this problem. The unit captures a high resolution image of the front and back of the ID card and extracts the data on any magnetic stripes. The image and related data will be transmitted to a forensic laboratory where a certified document examiner can conduct an analysis to determine the authenticity of the identification. When the examination is completed, the results are transmitted back to the remote image card unit. A process

that used to take a minimum of several days can now occur in less than an hour. The unit is small enough to easily fit on a countertop and requires little time to learn to operate.

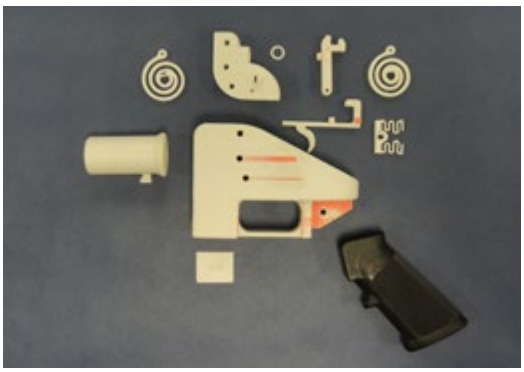


Mobile Data Triage, Ingest, and Search Tools

The law enforcement and intelligence communities extract or collect huge amounts of data from all types of mobile devices. Although this information is extremely useful, the data must be quickly and thoroughly analyzed or the validity and value of the data can be lost. Systems Engineering Technologies Corporation (SyTech) of Alexandria, Virginia has developed a tool that collects data which has been extracted from mobile devices. Once collected and stored, the data is automatically normalized, analyzed, and searched. The operator can preset the names, keywords, locations, addresses, cell towers, and other data items which the tool will search for and find. The tool then links and associates the data with any other information stored in the database. The tool can also automatically send email alerts to anyone who needs the information. This instant triaging of the data ensures that the evidentiary and intelligence value is not lost and provides the maximum amount of reaction time to the users.

Investigative and Forensic Analysis of 3D Printed Polymeric Firearms

Recent technological advancements have made it possible for firearms to be made through computer 3D printing composed of non-metallic materials such as ceramics, plastics, nylon, and polymeric materials. This is dramatically changing the investigative and forensic analysis of firearms and their related examinations. Applied Research Associates, Inc. of Littleton, Colorado, has investigated how these 3D printed polymeric firearms may have to be analyzed and examined differently from the presently used forensic techniques and procedures. Several 3D printed firearms were constructed and test fired to determine the different ballistic effects. After test firings, gunshot residue samples were collected and latent fingerprint processing techniques employed. Other examinations that were performed included DNA analysis and bullet comparisons. The results were compiled in a report which documented the test data and best techniques to utilize when analyzing 3D printed firearms.



DNA Radar

DNA evidence found at the scenes of terrorist and criminal activities is quite valuable in identifying who was present at the location. Typically, an individual's DNA profile, based on 13 standard core loci, must be in a database to establish their identity. However, using the information available from the remaining regions of the DNA can provide other identifying information including ethnic and familial traits. Kailos Genetics, Inc. of Huntsville, Alabama, has developed a DNA Radar system that harnesses a powerful sample preparation technique which can enable multiplexing of a large number of genetic regions for sequencing of minute amounts of DNA. The data is processed by a series of algorithms built on the advanced technology of human genetics. Valuable investigative leads are extracted from the samples even when the donor's profile is not in a database. Some of these leads involve inferences of surnames from male samples, ancestry information, and some phenotypic information such as eye color, hair color, and blood group predictions. Although full identification may not be possible, significant information and leads can be generated that can ultimately lead to a positive identification.

Advanced Automated Document Analysis Tool

A critical operation in many criminal and terrorist investigations is extracting information from counterfeit and fraudulent documents, especially those used for identification and travel. Linking the traits and features of these counterfeit documents provides valuable intelligence and investigative leads. This information can include the location where the documents were made, who may have created them, other crimes and operations in which they have been used, and when they might have been produced. Sphere of Influence, Inc. of McLean, Virginia, has developed an encompassing system that can quickly store and categorize the irregular traits and features on counterfeit documents. The system will automatically analyze and compare the traits and link them to other documents and investigations. This linking can connect documents to larger families of counterfeit documents and other investigations. The system contains barcode reading and optical character recognition capabilities, and the ability to recognize common image artifacts on multiple documents. Additionally, it can store images of the scanned fraudulent documents for later use and comparison.

ONGOING PROJECTS

Vehicle Image Search Tool

Forensic video and image analysis plays a key role in many combating terrorism operations. It can provide significant intelligence value, particularly through the comparison and identification of vehicles. Searching through vast amounts of video files to find and identify vehicles is difficult and extremely labor intensive. SRI International of Princeton, New Jersey, is developing an automated system that can rapidly search a wide range of multimedia video files to locate vehicles. The tool will provide post-event forensic analysis of video and digital image depictions and files. The system will automatically extract vehicle images from a range of multimedia digital image files in real time. It will have the ability to identify a vehicle's make and model and will associate and match individual vehicles to those stored in its image database. The system will also allow users to highlight or delineate key features to improve searching and matching performance, and will work on commonly used computer hardware.

Next Generation Vampire (Collaborative Forensic Exploitation Platform)

The U.S. military, law enforcement, and the intelligence community have a critical requirement for fast, efficient, and accurate collection and analysis of information, evidence, and biometrics from sensitive sites and crime scenes. Military and law enforcement personnel need equipment that is not redundant, supports multiple capabilities and requires minimal training time to employ. Booz Allen Hamilton of McLean, Virginia, is developing a rugged device weighing less than 2.5 pounds that will meet this requirement. Specific features include a 12-megapixel camera that can capture images of latent prints and full crime scene photos. It will illuminate the scene with white light and two ultraviolet light wavelengths as well as having a laser-based image rescaling system. The devices

will also capture live fingerprints from persons of interest. The units will include customized software that performs some analysis on fingerprint images and will be able to connect to databases including the FBI Next Generation Identification system. It will have the communication capability to form an ad hoc mobile network and share data with other Vampire units. Some facial recognition and document exploitation capabilities will also be available.

Heroin Origin by High Resolution Inductively Coupled Plasma-Mass Spectrometry

Terrorist organizations and criminal enterprises use the production and sale of heroin and related opium products to obtain huge amounts of revenue to fund their illegal and violent activities. When law enforcement or intelligence agencies collect or seize heroin or opium, it is far from the site where it was cultivated or processed. Determining its location of origin provides valuable intelligence for law enforcement and the intelligence community. Florida International University (FIU) in Miami, Florida, is developing forensically validated procedures to measure trace elements and isotope ratios of samples of heroin and its related products to determine the geolocation of their origin. They will use the most accurately known and readily available method to measure isotope ratios which is high resolution inductively coupled plasma-mass spectrometry (ICP-MS). Once the trace elements and their isotope ratios are measured, they can be compared to reference samples to accurately determine where the opium poppies were grown. FIU is also establishing an accompanying reference database that can be used to determine the origin of heroin as being from Mexico, South America, Southwest Asia, or Southeast Asia. The procedures developed will be able to analyze street heroin and opium samples as small as 400 milligrams with 95 percent accuracy.

Anomalous Workplace Behavior Intervention

Abnormal conduct, irregular actions, or unusual behavior patterns by persons in the workplace may be indicators of an insider threat. These actions can be a forewarning of a person committing significant acts of sabotage, espionage, sensitive information theft or other malevolent insider activities. Other employees frequently observe behavioral indicators, but rarely report them to others within their organization or the authorities. The reasons vary, but include reluctance to cause trouble for another worker, lack of knowledge of insider threat indicators, or not knowing how to report their observations to someone who will take action. In this project, the Centre for the Protection of National Infrastructure in the United Kingdom is developing techniques and procedures that encourage and motivate employees to report observations that may indicate insider threat inclinations in others in the workplace. The focus is on establishing an understanding of employee perceptions of anomalous workplace behavior and ways employees might choose to intervene. This effort will also identify the barriers to employees reporting those behaviors and develop prototype staff awareness campaigns. The techniques will emphasize reporting and intervention methods that are unobtrusive and anonymous for the employees. The project will also develop procedures for management to take quick and decisive actions without bringing any attention to the reporting person. Additionally, separate training programs for the workplace will be created to educate both employees and management.

MEMBERSHIP

Environmental Protection Agency

- National Enforcement Investigations Center

Federal Reserve Board

Intelligence Community

National Forensic Science Technology Center

National Transportation Safety Board

U.S. Department of Commerce

- National Institute of Standards and Technology, Office of Law Enforcement Standards

U.S. Department of Defense

- Component Commands
- Defense Advanced Research Projects Agency
- Defense Computer Forensics Laboratory
- Defense Criminal Investigative Service
- Defense Cyber Crime Institute
- Defense Forensic Enterprise, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
- Defense Forensic Science Center
- Defense Forensics and Biometrics Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Headquarters, U.S. Marine Corps
- Intelligence Systems Support Office
- Joint Improvised-Threat Defeat Organization
- National Center for Credibility Assessment
- National Geospatial Intelligence Agency
- National Media Exploitation Center
- Naval Research Laboratory
- Office of the Provost Marshal General
- Pentagon Force Protection Agency
- Rapid Reaction Technology Office
- U.S. Air Force Office of Special Investigations
- U.S. Army Criminal Investigation Command
- U.S. Navy Naval Criminal Investigative Service
- U.S. Special Operations Command

U.S. Department of Energy

- Office of Security Technology and Assistance

U.S. Department of Homeland Security

- Customs and Border Protection
  - Border Patrol
- Federal Emergency Management Agency
- Immigration and Customs Enforcement
  - Homeland Security Investigations Forensic Laboratory
- National Protection and Programs Directorate
  - Federal Protective Service
- Science and Technology Directorate
  - Transportation Security Laboratory
- Transportation Security Administration
- U.S. Secret Service

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- National Institute of Justice
- U.S. Marshals Service

U.S. Department of State

- Bureau of Counterterrorism and Countering Violent Extremism

U.S. Department of Transportation

- Federal Aviation Administration

U.S. Postal Inspection Service

IRREGULAR WARFARE AND EVOLVING THREATS

iwetsubgroup@cttso.gov

FOCUS AREAS

Advanced Influence and Information Capabilities

Conduct research, operational analysis, capability design, and implementation support to develop new tools, techniques, and activities that enable our forces to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries within the physical, information, or cognitive domains of the information environment.

Counter-Network Concepts and Capabilities

Conduct research, analysis, and development of new concepts and capabilities that integrate unique skill sets of combined, multi-agency and multi-national domains to identify and interdict threat networks and enterprises.

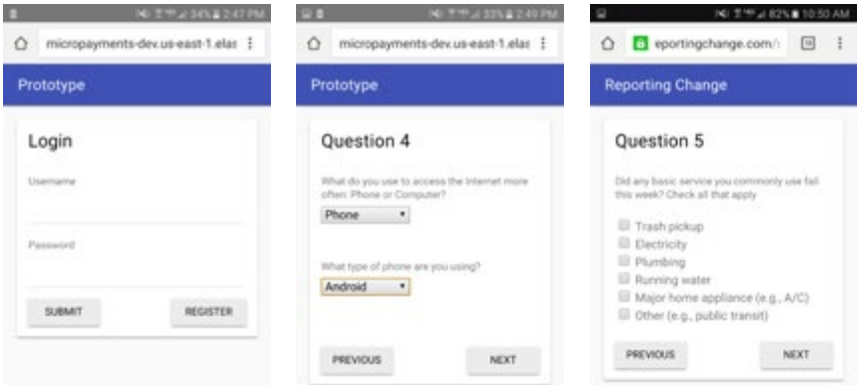
Partnership Capacity Development

Conduct research, operational analysis, capability design, and implementation support in order to more effectively assist, train, advise, and influence foreign partners, foreign competitors, adversary leaders, and relevant populations in support of expeditionary, low-cost, small-footprint operations in the air, land, maritime, and cyber domains.

COMPLETED PROJECTS

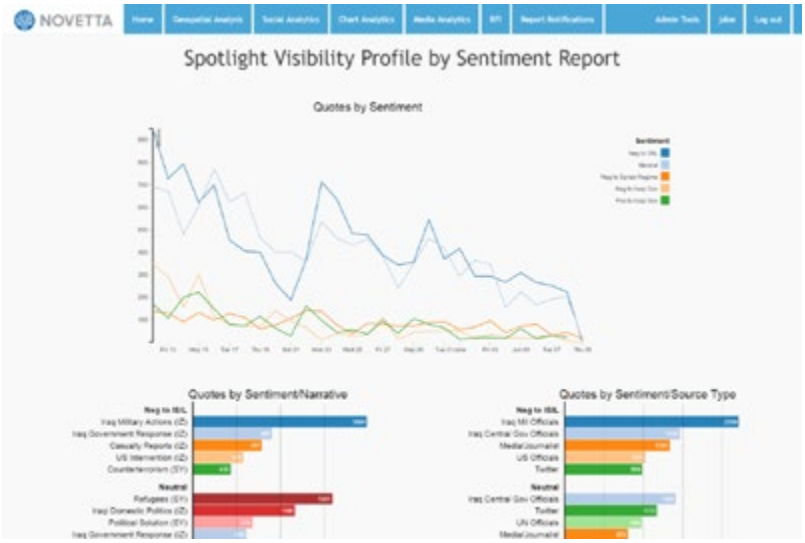
Micropayments in Support of Civil Reporting

Several emerging technologies, including micropayments, gamification, and blockchain, offer new approaches for encouraging civilians in conflict zones to provide information. This effort was initiated to develop an operational concept and application process that enables these civilians to be quickly rewarded with "tip-sized" amounts of virtual currency when they share information about their local environment. A field test was conducted to determine the functionality of this method as a next generation survey activity—one that is culturally optimized, incentivized, and easily accessible. This approach to civil reporting may form the basis for collecting more varied atmospherics in other geographic areas.



Spotlight

As the threat environment continues to shift, new and expanded requirements have emerged. This includes leveraging non-traditional data sources and using information as a strategic layer of conflict. Spotlight was initiated to increase the analyst's ability to monitor, analyze, assess, and respond to changes in the operational information environment. In addition to exploiting adversary vulnerabilities in the information and physical domains, Spotlight also uses new data (including human rights, incidents of violence, and frequency of atrocities), to identify patterns of tactical behavior by state and non-state actors.



Whole-of-Government Approach to Address Future Transnational and Trans-regional Capacity

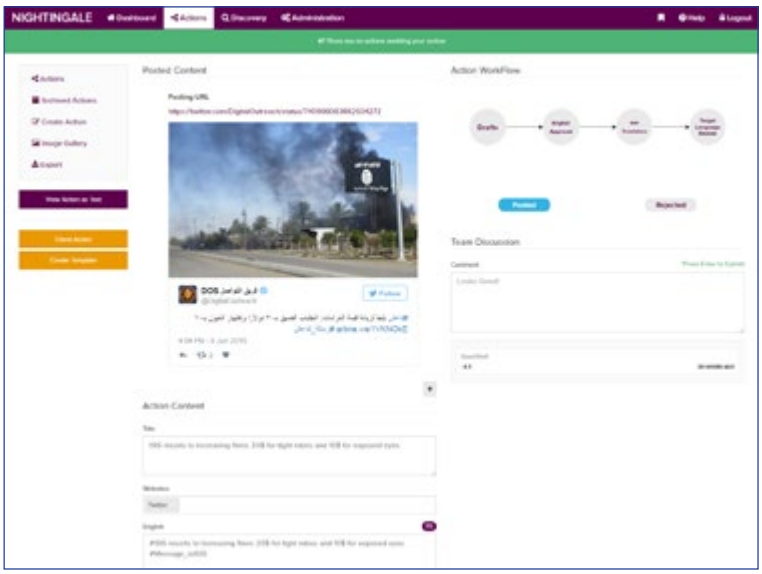
Since the 9/11 attacks, U.S. interagency leaders have faced a complex, unstable international security environment, no longer defined by the state aggressors of past conflicts. As the last combat forces withdraw from Afghanistan, a new hazard is looming on the horizon. The global threat is a hybrid of disruptive agents, converging to represent international disorder, and requiring a "re-posturing" of U.S. national security policy that places greater emphasis on early phases of planning. To this end, this project conducted an analysis of existing programs supporting U.S. investment in transnational and trans-regional capacity building missions. This effort delivered an analysis of the measures of effectiveness of existing authorities and an initial roadmap for extracting greater value from current and future interagency collaboration. The final report delivered recommendations on developing the capacity necessary to counter a global blended threat in an increasingly constrained fiscal environment.

ONGOING PROJECTS

Expeditionary Information Operations

Our adversaries have demonstrated skill using communications technology across domains, including information-related capabilities, to conduct hybrid-warfare. By operating beyond physical battlegrounds, they are able to subvert our efforts by using propaganda and disinformation to affect public perceptions. Now, more than ever, we must be aware of the information environment. This project seeks to understand the information environment in 2025, outline potential capability gaps, and describe actions to help gain and maintain information dominance. In addition, it explores information-related capabilities of defense agencies, emerging technologies, and recommends implementation strategies based on current budget concerns.

Nightingale



Engaging in social media and countering messages of the Islamic State in Iraq and the Levant (ISIL) and likeminded terrorist organizations is no longer an option but a necessity. Nightingale seeks to coordinate, inform, and expand messaging capabilities in support of countering violent extremism (CVE), specifically propaganda and misinformation. This includes mission-enabling products, such as workflow processes and expanded analytics, to strategically engage foreign audiences. The Nightingale effort has increased efficiency by streamlining approval and archiving processes, providing situational awareness, and improving collaboration capabilities. Much of this development was based on iterative feedback directly from operators, which has enabled programmers to provide quick-turnaround releases that address high priority needs. Nightingale can be leveraged by other elements of the U.S. Government that are also actively participating in counter messaging. Future objectives for Nightingale include expanded analytics, metrics, threat reporting, and new tools for information sharing across the U.S. Government, with foreign governments, and non-governmental partners.

Secure Unclassified Network

The Secure Unclassified Network (SUNet) is an accredited web-based platform providing a "whole-of-nations" secure, operational infrastructure for multi-agency users (law enforcement, interagency, coalition, and foreign nationals). This agile platform has the ability to segment users, data, and tools. As such, SUNet creates an otherwise unavailable capability for traditional and non-traditional mission partners to share data, collaborate, have secure email, and share/access advanced analytic tools. Unlike standard commercial systems, SUNet has been accredited by the U.S. Government under the DoD Information Assurance Certification and Accreditation Process (DIACAP) and has received a "GIG Waiver" from the Department of Defense Chief Information Officer on the grounds that it provides a unique capability that is not currently available in the Defense Information System Network. Most recently, SUNet has been leveraged to provide web-based situational awareness and analytic capabilities via an accredited plug-and-play platform enabling users to apply the best data and applications needed to characterize and geospatially visualize the information environment for operational level planning and a range of tactical missions.

Behavioral Influence Assessment

The Behavioral Influence Assessment (BIA) project is a joint endeavor between Sandia National Laboratories and the Defence Science and Technology Laboratory, United Kingdom Ministry of Defence. Using expert knowledge, social science theories, modeling, and research-driven data, the project seeks to understand the reactionary behaviors of violent extremist groups in response to potential courses of kinetic and non-kinetic actions or events — specifically when it comes to planning and conducting operations in support of foreign partner nations. This effort explores the way specific actions influence or elicit a desired response among internal and external entities. Upon completion, it will serve as a Phase 0 planning tool for analysts seeking to understand the cascading influences and reactions to events which would have previously been difficult, if not impossible, to forecast.

MEMBERSHIP

Intelligence Community

National Defense University

United Kingdom

- Strategic Analysis Group – Policy and Capability Studies

U.S. Agency for International Development

U.S. Department of Defense

- Coalition Joint Forces Land Component Command
- Combined Joint Task Force
- Defense Institute of Security Assistance Managemen
- Peacekeeping and Stability Operations Institute
- Strategic Capabilities Office
- U.S. Army
- U.S. Army War College
- U.S. Central Command
- U.S. European Command
- U.S. Southern Command

U.S. Department of Homeland Security

- Office of International Affairs

U.S. Department of Justice

- International Criminal Investigation Training Assistance Program
- Federal Bureau of Investigation
  - Global Training Unit
  - Instructional Systems
- Office of Overseas Prosecutorial Development Assistance and Training

U.S. Department of State

- Bureau of African Affairs, Office of Regional Security Affairs
- Bureau of Counterterrorism and Countering Violent Extremism
- Bureau of Educational and Cultural Affairs
- Bureau of Political-Military Affairs
- Global Engagement Center

U.S. Department of the Treasury

- Office of Terrorism and Financial Intelligence

U.S. Patent and Trademark Office

Wilson Center

- Africa Program

PERSONNEL PROTECTION

ppsubgroup@cttso.gov

FOCUS AREAS

Communications and Situational Awareness

Develop situational awareness and communication capabilities that aid in identifying threat indicators, conducting risk assessments and providing early warning to personnel providing protective services for VIPs. Develop tools to facilitate situational awareness, reporting, and communications for incident response personnel.

Individual Protection and Survivability

Develop advanced personnel protection systems that mitigate ballistic, blast, and emerging operational threats. Personal protective equipment focuses on novel materials and designs to provide maximum protection.

Personnel Tracking and Recovery

Develop inconspicuous systems to geolocate and track high risk personnel, signal situations of duress, and facilitate recovery of missing or captured personnel.

Ballistic and Blast Threat Assessment

Research ballistic and blast effects on the human body and develop guidelines, tools, and techniques to mitigate the effects.

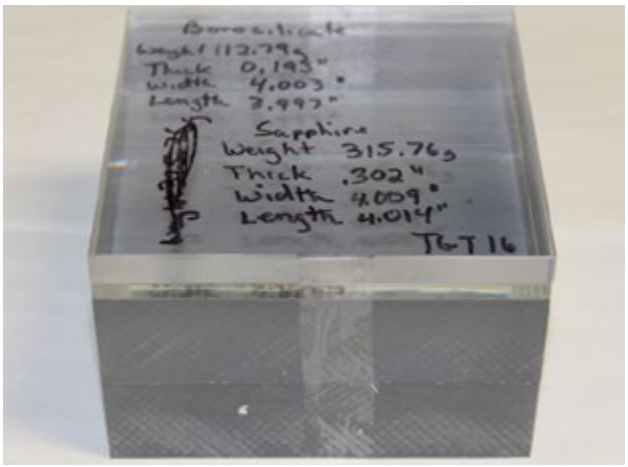
COMPLETED PROJECTS

Ballistic Clay Characterization

There is concern that existing test methods to characterize body armor may not accurately describe the level of performance afforded to the user. Body armor performance is partially dependent on the contact of the armor against the body. One of the test methods that measures backface deformation uses flat clay blocks and does not take into account inherent anatomical differences between genders, nor within gender differences in physique. To assess whether or not the technique using clay blocks could be modified to gain more realistic performance data, HP White Laboratory, Inc. conducted a study in which the clay test blocks were built to more realistically represent gender and physique anatomical variations. Data from this study was provided to the National Institute of Standards and Technology for analysis and potential use in the development of future body armor test standards.

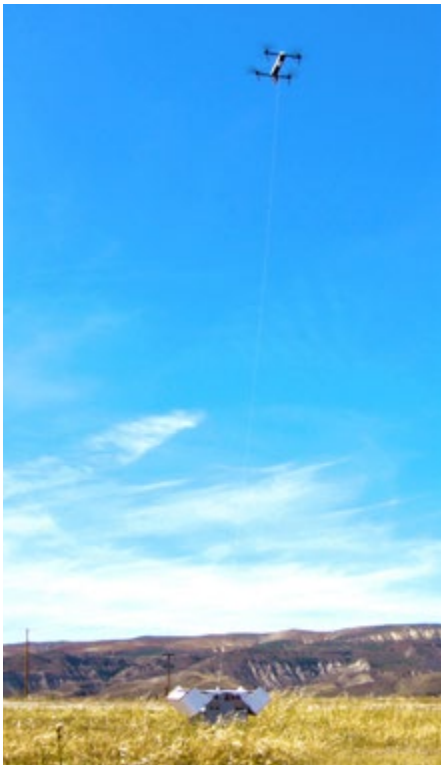
Ballistic Face Shield

Tactical operators often participate in raids requiring forced entry into facilities. The first person through the door is, at least momentarily, the lone target of enemy resistance until joined by the rest of the team. A breacher's center mass is well protected by body armor, but there has been little development in ballistic protection for the head, neck, and face. The Naval Research Laboratory (NRL) worked on two approaches to develop one element of a head and face protection system. One approach integrated contemporary, ceramic, ballistic materials into an opaque face shield for the enhanced combat helmet. This face shield is opaque and eliminates vision, so the effort also developed a zero latency vision system which will project the operator's normal field of vision to the inside of the shield, preserving and possibly enhancing situational awareness.
The second approach developed a novel recipe of transparent armor into an enhanced combat helmet. NRL has recently been awarded a patent for this innovative combination of materials. This effort has provided a vital step forward in head protection for tactical operators.



Micro LTE

Use of unmanned aircraft systems (UAS) to observe or collect video of specific targets/areas has proven to be a valuable tool in a wide variety of field operations. However, the camera feed is only visible by those at the control station. Field operators must rely on critical information being relayed to them from those observing the feed. Raytheon Blackbird Technologies, Inc. of Herndon, Virginia, has developed the Micro-LTE Single Channel Device which provides not only the ground control station, but also field personnel a common operating picture via their cellular devices such as mobile phones and tablets. The Micro-LTE is a small device designed for quick and easy installation into Tier 1 UAS. It can transmit over the commercial 4G LTE cellular network as well as a private 4G LTE cellular network controlled by the end user to send encrypted video data to field operators' cellular devices. The system uses its own power supply which lasts approximately two hours and can provide video data to eight users. The system is compatible with commercial-off-the-shelf 4G LTE smart cellular devices and is ruggedized to withstand the same environmental conditions in which the UAS operates. The capability has been successfully demonstrated and delivered to the Department of State for operational test and evaluation. There is also interest from military components to operationalize this technology for enhanced situational awareness.



Tether Eye

Government agents deployed in austere locations have limited means for communications and intelligence, surveillance, and reconnaissance (ISR) capabilities. Current small unmanned aerial vehicles (UAVs) lack the endurance and payload capacity to satisfy extended ISR flight times and communications in potentially hostile situations. Tether Eye, developed by AeroVironment, Inc. of Simi Valley, California, is a tethered UAV solution that solves this problem by providing a UAV that can be transported in small vehicles, carried by two people, and set up quickly. The system can be powered from AC shore power or DC power. The launch and recovery system (LRS) supplies power to the UAV through the tether system, and the UAV can remain airborne indefinitely. The UAV can be deployed immediately after set up or staged for a delayed launch for which the LRS provides environmental shelter until the system is commanded to deploy. Once deployed, the UAV climbs to a maximum altitude of 150 feet above the LRS in less than one minute. The deployment altitude may be pre-set by the operator at any altitude between 40 and 150 feet above ground level. The UAV automatically holds a position above the LRS. Tether tension and the UAV altitude are adjusted automatically to compensate for unpredictable wind conditions including gusting. The UAV ISR payload includes a real-time video capability. The system operator directs the payload through the ground control station (GCS) touch screen display and has the ability to scan the area 360 degrees continuously. The operator can lock on a selected object and has the ability to zoom in if required. An infrared camera is provided in the payload for night situational awareness. Video image

is displayed on the GCS and through an interface to a remote control center. The communications relay function is performed either by the digital data link Ethernet bridge function, or by a customer provided radio-relay payload that replaces the ISR payload. Recovery of the UAV to the LRS is initiated by the user and is performed automatically. Backup batteries in both the LRS and UAV provide emergency power in case of main power interruption or tether breakage. In the event of power loss, the UAV will automatically recover to the LRS or to a designated landing site. Five systems have been delivered for operational test and evaluation in the United States and overseas with military and government agency end users.

ONGOING PROJECTS

Counter UAV

Unmanned aerial vehicles (UAVs) or "drones" have entered the commercial market space and are readily available to consumers via the internet. The ease of use and accessibility to this powerful technology has drawn attention to the potential harmful uses of UAVs. Many incidents have occurred in recent history where drones have been flying in unauthorized locations and creating potentially dangerous situations. In many cases, the UAV operators are not operating with malice; however, flying in unauthorized areas does cause concern for the safety of personnel and aircraft in the area. In order to protect U.S. personnel and facilities, CTTSO is conducting several projects that will identify and better characterize problems that can be posed by UAVs. Additionally, CTTSO is investing in technologies that detect and mitigate the problems that UAVs can potentially pose. The goal is to develop a suite of technical solutions that can be tailored to the operating environment in which they will be used. As part of the project portfolio, different mitigation techniques are under consideration with a focus on non-kinetic technical solutions.

Enhanced Vehicle Tracker

Global Positioning System (GPS) deprived or denied environments are prevalent in high risk areas in which vehicles travel and lose reception to location servers. Raytheon Blackbird Technologies, Inc. of Herndon, Virginia, is developing the Enhanced Vehicle Tracker (EVT), a vehicle embedded device, which employs a means to track the location of a vehicle within 15 meters for a minimum of 30 minutes when the GPS is lost. The EVT employs an adaptation of a Raytheon Blackbird tracking and communications module, SmartCore™, as the basis for the EVT device. The EVT operates through a layered approach using both absolute position references and position estimating techniques to maintain accurate vehicle positions. Absolute position references and position estimates are obtained, respectively, by using radio frequency (RF) signal trilateration from cell towers and Wi-Fi emitters and by using the device's inertial measurements and information about vehicle motion from the Onboard Diagnostics

(OBD2) port. The data collected is transmitted to a remote Fusion server established specifically for this device and is processed, analyzed, and prioritized to assess errors and correlate information to provide an accurate location of the vehicle to a command center operator. The system is designed to operate effectively under differing operational scenarios where tracking capabilities are interfered with or jammed through RF interference or physical obstructions. The EVT will provide location data within four minutes of the vehicle's engine start and if the GPS is lost, the EVT will enable command center personnel to maintain the vehicle's location for enhanced situational awareness and incident response capabilities.

Event Pin Identification System

Federal agents are assigned a set of event pins to designate their participation in major interagency events. Command post officers perform a visual pin inspection to identify approved personnel. This raises security concerns if a pin is lost, stolen, or duplicated with high fidelity. Impact Research and Technology, LLC of Phoenix, Arizona is developing the Event Pin Identification (ID) System to mitigate this security concern and assist in agent recognition. The Event Pin ID System integrates long-range passive radio frequency identification (RFID) technology, secure network server, and custom database software to discretely detect event pins. An Event Pin assigned to each protective service agent will contain that agent's personal information and be displayed on an Event Pin ID System for a command post officer's review. Upon entry to a venue, the system will provide the command post officer with the agent's name, photograph, physical description (i.e., height, weight, eye color, etc.), and pin status for visual comparison. Invalid tags and unauthorized agents trigger visual and audible alarms to alert command post officers of a potential security breach. Additionally, the system will be capable of distinguishing between an agent entering and exiting a post, and the system will have a minimum detection range of 30 feet. Agent identifying information contained within the database and communicated across servers is secured by a security system employing AES 256-bit encryption. The Event Pin ID System will be used to facilitate improved security over visual pin inspection to identify approved and unapproved personnel during large interagency events.

Used Armor Response Corridors

Law enforcement, military personnel, and protective details perform their tasks in many environmental conditions and climatic regions. Each region has a unique climate that contributes to the lifecycle of body armor. Extreme heat, moisture, and frigid temperatures are some of the factors that could affect the longevity of personal armor. Each duty performed by personnel, storage conditions, laundering schedule, and general care can all have cumulative effects on the lifecycle of body armor. Armor manufacturers recommend a service life of five years based on a generalized, average lifecycle. This project seeks to validate the recommended service life across the various environments and duty uses seen by law enforcement personnel. In this effort, HP White Laboratory, Inc. will collect hundreds of armor types from federal, state, and local law enforcement through voluntary donation of out of service armor. Each piece of armor will be evaluated on its condition, use history, model number, protection level, duty use, and other variables. The armor will be tested to determine the ballistic limit of the armor in the used condition. HP White Laboratory, Inc. will compile the test data and historical data of the armors to determine what lifecycle conditions contribute to any demonstrated performance degradation seen in the tested armors. Results will be used to craft recommendations for storage and care protocols and inform procurement cycles for the government.

MEMBERSHIP

Intelligence Community

U.S. Capitol Police

U.S. Department of Commerce

- National Institute of Standards and Technology
- Office of Law Enforcement Standards

U.S. Department of Defense

- Defense Threat Reduction Agency
- Joint Personnel Recovery Agency
- Pentagon Force Protection Agency
- Rapid Reaction Technology Office
- U.S. Air Force
  - Office of Special Investigations
- U.S. Army
  - Criminal Investigation Command
  - Joint Trauma Analysis and Prevention of Injury in Combat
  - Medical Research and Material Command
  - Natick Soldier Systems Center
  - Program Executive Office Soldier
    - Soldier Protection and Individual Equipment
  - Research, Development, and Engineering Command
  - Research Laboratory
  - Tank Automotive Research, Development, and Engineering Center
- U.S. Navy
  - Naval Air Systems Command
  - Naval Criminal Investigative Service
  - Office of Naval Research
  - Program Executive Office, Ships
- U.S. Special Operations Command
  - Army Special Operations Command
  - Marine Corps Forces Special Operations Command
  - Naval Special Warfare Command

U.S. Department of Energy

U.S. Department of Homeland Security

- Customs and Border Protection
- Federal Law Enforcement Training Center
- Transportation Security Administration
  - Federal Air Marshal Service
- U.S. Secret Service
  - Special Services Division, Technical Security Division

U.S. Department of Justice

- Federal Bureau of Investigation
- National Institute of Justice

U.S. Department of State

PHYSICAL SECURITY

pssubgroup@cttso.gov

FOCUS AREAS

Blast Effects and Mitigation

Evaluate blast threats and develop anomaly detection and mitigation approaches to protect groups of personnel, facilities, installations, and venues. Develop decision support tools and technical solutions related to blast effects.

Screening, Observation, Detection, and Protection

Develop technologies and techniques to protect personnel in facilities, and infrastructure, by improving situational awareness; detecting, identifying, and locating threats; and, controlling access to critical assets. Emphasize automatic threat detection/alerting.

Maritime Security

Develop technologies to protect ships, ports, shore and offshore facilities. Develop sensors and devices for detection and tracking; physical barriers; and stopping devices.

Subterranean Activities

Develop capabilities to detect, locate, map, monitor, survey, and disrupt subterranean infrastructure and activities in permissive and non-permissive environments.

COMPLETED PROJECTS

Temporary Anti-Personnel Barrier

Over the past decade there have been a number of threats to U.S. overseas facilities from angry mobs and violent crowds. To counter this threat there is a need to temporarily increase perimeter standoff and add layers of defense on short notice. To meet this need, the Temporary Anti-Personnel (TAP) Barrier System, a field-deployable, enhanced crowd control measure, was developed to protect high value targets such as embassies and consulates against hostile personnel. The TAP Barrier System is rapidly deployable with a configurable modular assembly that allows

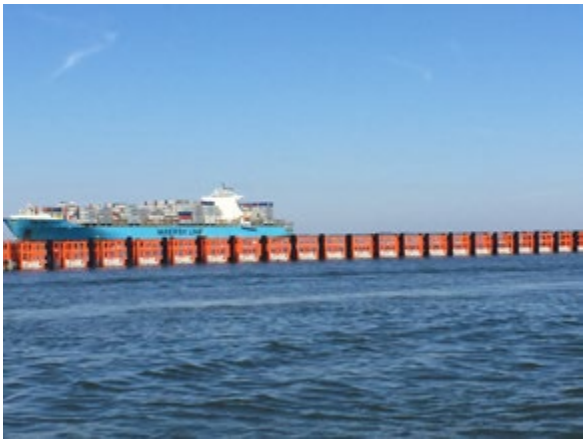
Images courtesy of Mitigation Technologies

TAP Barrier is versatile and configurable

a user to navigate real-world topography. It can be stored and shipped in a standard ISO container, and stands 9-feet tall with the option of increasing to ten feet with anti-climb spikes. The barrier is capable of delaying or deterring hostile personnel that may attack it with locally available implements, such as sticks, rocks, and hammers, allowing U.S. personnel the opportunity to conduct directed courses of action (i.e., marshaling, egress, destruction of classified material, etc.). Though the initial use is intended for overseas facility protection, the system has many features that could also support domestic law enforcement.

Next Generation Port Security Barrier

Waterside security continues to be a U.S. Navy force protection priority. The current port security barrier (PSB) is part of a class of barriers referred to as net-capture or Type I barriers. Fleet experience with this PSB design has yielded recommendations for a next generation (Type II) barrier. The U.S. Navy has been conducting tests and evaluations of a commercial-off-the-shelf water barrier system, manufactured by HALO Maritime Defense Systems, that provides increased protection against small boat attacks in a reduced footprint and at a lower lifecycle cost. HALO system configurations and mooring plans can be tailored to the force protection goals of the customer and the specific characteristics of the site to be protected. Configurations typically include a combination of a static double-wall barrier and a remotely operated gate.

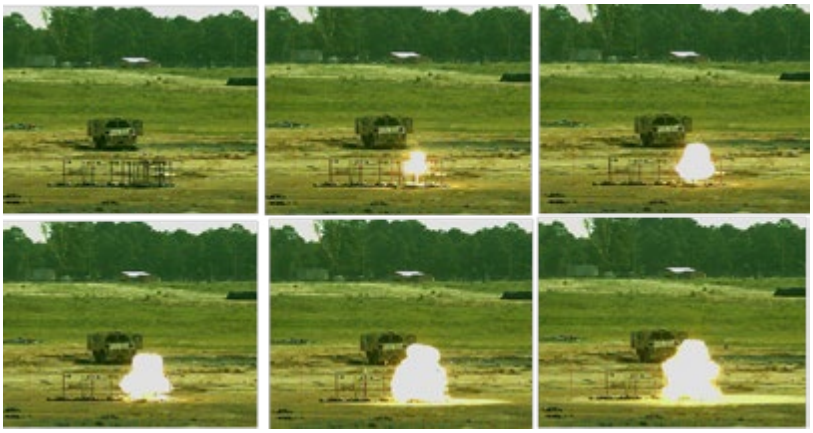


HALO Guardian™ gate, Naval Station Norfolk, Virginia

Under a CTTSO contract, a HALO system, consisting of a 300-foot Guardian™ gate attached to two Sentry™ support platforms, successfully completed a long-term, operational and environmental test and evaluation at Naval Station Norfolk, Virginia. Over an eight-month period spanning fall and winter, the HALO system underwent monthly evaluations of the semi-automated

gate's opening and closing capability; system resilience, structural integrity, and connection strength; and effects of weather, waves, and currents on HALO system components. Data collected from this test will inform follow-on U.S. Navy-sponsored tests and a major acquisition decision on Type II barriers for maritime force protection of critical assets at domestic and overseas bases.

Novel VBIED Characterization and Modeling



Images courtesy of ERDC Test Range (Sponsored by CTTSO)

In recent years, there has been a proliferation of online how-to guides and literature posted by terrorist groups and other antagonists that provide detailed instructions for building homemade explosive devices using common household items. To ensure security forces, first responders, and emergency planners have the tools and information they need to plan for, prevent and respond to these homemade threats, CTTSO, in collaboration with Australia's Defence Science Technology Group, conducted a project to test, assess, evaluate, and create a model library for a specific vehicle-borne improvised explosive device (VBIED) mentioned in multiple terror magazines. This threat model has been incorporated into the Defense Threat Reduction Agency's Vulnerability Assessment and Protection Option (VAPO) software to analytically determine and visually understand explosive effects on humans and infrastructure. This will allow for more accurate and realistic pre-event planning, training, and emergency response actions.

Screenshot from RCP Software

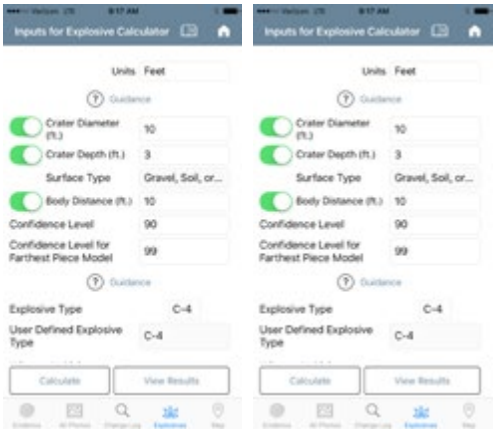
Rapid City Planner

Rapid City Planner (RCP) is a predictive, explosive modeling software that is the result of a joint project between CTTSO and Defence Research and Development Canada. It has an easy-to-use interface that can be used by professional blast engineers or first responder emergency planners to accurately model an urban explosive event. RCP has the ability to run high-fidelity computational fluid dynamic (CFD) codes 50 times faster than previous codes. Through a fundamental rewrite of CFD calculations that take advantage of GPU processing, explosive modeling can be accomplished in hours as opposed to days. The increased speed of RCP does not impact the accuracy of the models and by incorporating an embedded Google application models can be run for specific locations. Licenses for RCP have been provided to a number of agencies that oversee emergency management, operations planning, and first responders. All are planning to use RCP to support security assessments of high visibility public events. Additional licenses can be purchased from Martec Limited, a member of Lloyd's Register group, along with user support packages.

Tactical Aerostat (Light Eye)

CTTSO in partnership with the Israel Ministry of Defense (IMOD) developed a compact, maritime and ground, tactical aerostat surveillance system. The ground variant is designed for day or night intelligence, surveillance/reconnaissance applications, and communication between non-line-of-sight ground forces. Both systems include day or night observation payloads, a laser pointer, and a dual-purpose tether for both communications and energy feed from surface to platform. High quality aerial imagery with 360-degree coverage and a range out to 5 km is made possible through a unique electro-optic imaging device with 3-axis gyroscopic stabilization. The ground-based system is also equipped with a mobile ad hoc networking system. The Light Eye is capable of reaching altitudes of 800 m and can operate effectively in wind speeds up to 30 knots. The system is designed for easy mobilization and rapid deployment. Light Eye is transportable by two operators, deployable in 30 minutes, and can be launched and operated by a dismounted soldier from a small all-terrain vehicle or maritime vessel. The U.S. version contains an automatic deflation device that allows for aerostat descent in the event of a tether breakage. The maritime version was evaluated on a United States Coast Guard vessel to provide the capability to visually detect, identify, classify, and track small vessels that are beyond line-of-sight or over the horizon. The Israel Police and IMOD currently use a daytime version of the Light Eye.

Enhanced Vehicle Explosion Analysis Software (VExAS)



Terrorists continue to attack civilian and government targets with vehicle-borne improvised explosive devices (VBIEDs). VExAS uses algorithms based on VBIED blast tests to estimate scatter patterns of debris. These patterns are then used to focus searches for evidence in the most likely locations, document the evidence once found, and create a virtual layout of a post-blast scene. Under a bilateral effort with the Future Systems and Technology Directorate, Singapore Ministry of Defence, the VExAS desktop software was upgraded adding user-friendly application enhancements, and a mobile application was developed for both iOS and Android platforms. This has provided first responders and investigators a more capable tool to expeditiously, effectively, and efficiently process a post-blast scene.

ONGOING PROJECTS

Fixed Site Optical Radar for Tactical Outposts

Tactical teams have an ongoing operational need to enhance their situational awareness and to scan for potential threats to combat outposts in remote and potentially vulnerable locations. Currently deployed long-range observational platforms that assist in providing this situational awareness largely require manual operation by operators, thus demanding that valuable, high-demand manpower assets spend a significant amount of time and effort scanning for threats. This project is to design, develop, test, and deliver a Fixed Site Optical Radar

for Tactical Outposts (FSORTO) that will allow small tactical teams operating in austere locations to effectively scan the full 360 degrees of their perimeter for threats. The FSORTO will provide automatic observation and detection of threats at long distances, out to 18 km for vehicles and 12 km for personnel. The system will interface with Wave Relay® mesh network radios, enabling personnel to see the video on their handheld radios. The FSORTO will be lightweight, offer real-time video, and will consist of an electro-optical, two-axis, stabilized turret system containing a thermal camera and a daytime TV camera. It will also include a laser range finder, laser pointer, and differential GPS system to provide accurate target locations.

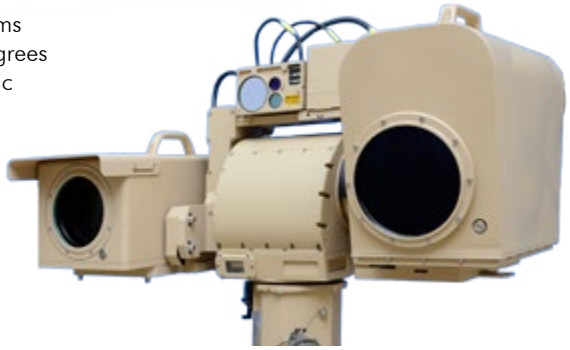


Image courtesy of Controp Precision Technologies LTD

Image courtesy of EMRTC for CTTSO

Enhanced Urban Canyon

CTTSO, in collaboration with Singapore's Defence Science and Technology Agency, is studying how blast propagates through a complex urban environment. City buildings are constructed with metal, glass, wooden or other facades that bend and break up during explosive events. These localized responses affect how blast pressures can vent, diffract, refract, and propagate through an urban environment. Understanding these factors is important to estimate the effect and range a particular explosive device will have in an urban environment, and will drive the enhancement of High Fidelity Predictive Blast Modeling (HFPBM) and Fast Running Models (FRM) software. Improved prediction of the urban blast environment will benefit security forces, first responders, and emergency planners that rely on these tools to plan for and respond to an explosive attack in high density urban centers.

Access Delay Systems

Yahya Arhab/European Pressphoto Agency

Domestic and overseas government facilities, or commercial sites which are critical, are increasingly at risk for targeted attacks by terrorists and other adversaries. The motivations vary from terrorists intending to harm personnel or destroy national icons, to state actors wanting to procure classified information and material. In both cases, additional countermeasures in place would delay an attacker from gaining entry, allowing first responders to arrive, classified materials to be destroyed, or facility personnel to egress to a safe location. CTTSO is collaborating with the United Kingdom's Centre for the Protection of National Infrastructure to investigate and test a series of access delay systems and combine various sensory disruption and access restriction technologies for use at sensitive locations where the threat of manual attack and hostile incursions on the facility is high. Though some access delay technologies are used in the public domain, most are intended to protect commercial businesses against attackers motivated by crime, not terrorism. This effort seeks to identify and test those technologies which have potential for use at high-risk facilities. Test results will be used to combine and integrate select technologies into access delay systems that will have maximum effect on potential attackers attempting illegal access to government facilities.

MEMBERSHIP

American Society for Testing and Materials

Environmental Protection Agency

Federal Reserve Board

General Services Administration

Intelligence Community

National Reconnaissance Office

State and Local Agencies

- DC Metropolitan Police Department
- DC Protective Services Police Department
- New York City Police Department
- Port Authority of New York and New Jersey
- Virginia Department of Transportation

U.S. Capitol Police

U.S. Department of Commerce

- National Institute of Standards and Technology

U.S. Department of Defense

- Defense Advanced Research Projects Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Explosives Safety Board
- Joint Chiefs of Staff
- Joint Improvised-Threat Defeat Organization
- Joint Non-Lethal Weapons Directorate
- Joint Task Force North (NORTHCOM)
- Joint Warfare Analysis Center (JFCOM)
- National Ground Intelligence Center
- Office of the Secretary of Defense
- Physical Security Enterprise and Analysis Group
- Unified Combatant Commands
- U.S. Air Force
  - Research Laboratory
- U.S. Army
  - Armament Research, Development, and Engineering Center
  - Army Research Laboratory
  - Asymmetric Warfare Group
  - Communications-Electronics Research, Development and Engineering Center
  - Corps of Engineers
  - Engineer Research and Development Center
  - Office of the Provost Marshal General
  - Night Vision and Electronic Sensors Directorate
  - Rapid Equipping Force
  - Research, Development, and Engineering Command
  - Training and Doctrine Command
- U.S. Marine Corps
  - Central Command
  - Systems Command
  - Warfighting Laboratory
- U.S. Navy
  - Chief of Naval Operations
  - Commander Navy Installations Command
  - Expeditionary Combat Command
  - Naval Criminal Investigative Service
  - Naval Explosive Ordnance Disposal Technology Division
  - Naval Facilities Engineering Command
  - Naval Facilities Engineering Service Center
  - Naval Sea Systems Command
  - Naval Undersea Warfare Center
  - Office of Naval Research
  - Strategic Systems Programs
- U.S. Special Operations Command
  - Army Special Operations Command
    - Army Special Forces Command (Airborne)
    - Joint Special Operations Command
  - Marine Corps Forces Special Operations Command
  - Naval Special Warfare Command
    - Naval Special Warfare Development Group

U.S. Department of Energy

- Federal Energy Regulatory Commission
- National Nuclear Security Administration
- Nuclear Regulatory Commission

U.S. Department of Homeland Security

- Customs and Border Protection
- Immigration and Customs Enforcement
- National Protection and Programs Directorate
  - Federal Protective Services
- Science and Technology Directorate
  - Transportation Security Laboratory
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of the Interior

- Bureau of Reclamation

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Federal Bureau of Prisons
- U.S. Marshals Service

U.S. Department of State

- Bureau of Diplomatic Security

U.S. Department of Transportation

- National Transportation Systems (Volpe Center)

SURVEILLANCE, COLLECTION, AND OPERATIONS SUPPORT

scossubgroup@cttso.gov

FOCUS AREAS

Biometrics, Recognition, Identity Intelligence, Tracking, and Exploitation (BRITE)

Improve technologies to identify and/or mask entities of interest using or countering biometrics, pattern recognition, database technologies, and exploitation methodologies.

Cyber and Convergence Technologies

Support or improve technologies for cyber and signals collection as these technologies increasingly converge with other systems and technologies to include, but not limited to the "Internet of Things."

Human Language Technology (HLT) and Media Exploitation

Develop and employ HLT where these technologies can best assist humans – operators and analysts – to make sense of volume and the variety of media sources; apply timely and actionable information in theater; and enhance communication skills and cultural understanding.

Surveillance/Counter-Surveillance

Develop audio, video, and advanced surveillance technologies, as well as automated tools and techniques to defeat adversarial tactics, techniques, and procedures, and methodologies.

Technical Collection/Special Communications

Improve ISR by developing and enhancing multi-INT sensors, SIGINT collection, and tagging tracking, locating technologies for intelligence operations. Develop and enhance special communications and canine advanced technologies in support of Special Operations and intelligence collection activities.

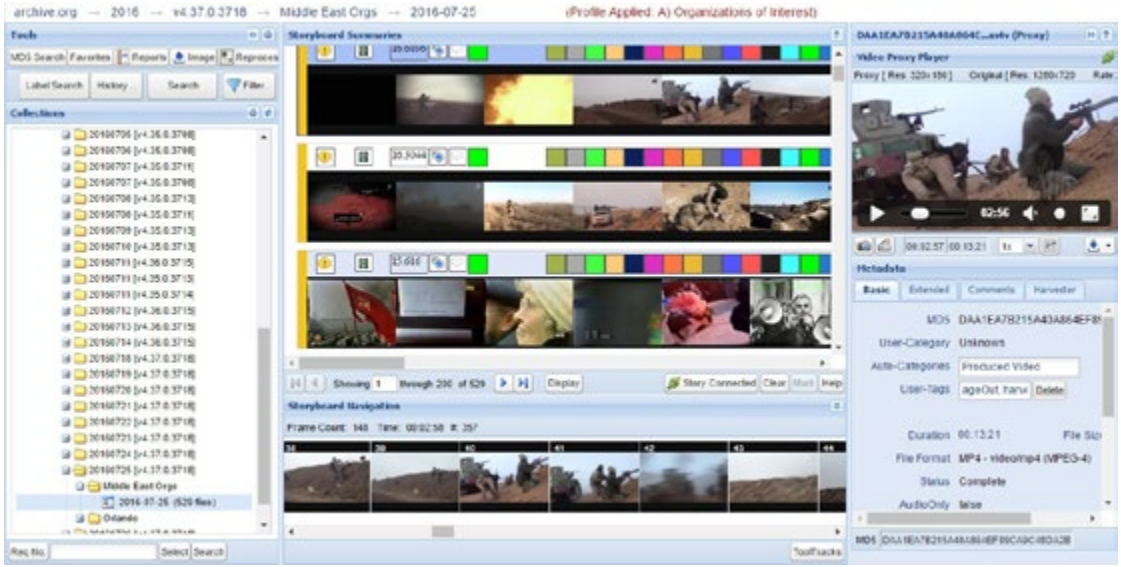
COMPLETED PROJECTS

Barnacle II

Barnacle II delivered Turkish language capabilities for multimedia exploitation and analysis of publicly available information from broadcast, web, and social media content. The project focused on acquiring, optimizing, and reconfiguring Raytheon BBN's commercial audio speech recognition engine, and subcontracting to SDL Federal Solutions, Inc., to create improved Turkish machine translation of formal and informal content. These new components were integrated into the latest Multimedia Monitoring System (M3S) application, providing media indexing, entity summaries, and social media channels to various government users who need access to Turkish data sources and analytic tools for operational missions.

Triage and Exploitation (TREX)

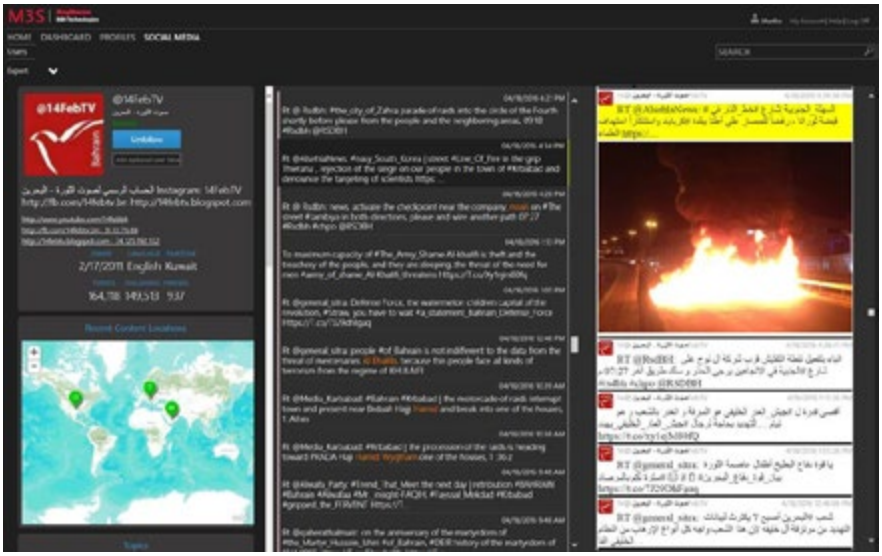
A quarter of the planet's population has video-capable smartphones, with the number and variety of devices collecting video growing rapidly. In order to process the extremely large and ever growing amount of images and media, Pixel Forensics, Inc. created the Triage and Exploitation (TREX) solution for media analysis. TREX enables



a user to rapidly discover critically important facts and evidence by automatically finding and visualizing high-value media from multiple devices and from a growing visual big data repository. TREX processes media files (videos, scenes, or frames) and presents them to the user in priority order based on user specified input, allowing them to rapidly find and review the relevant/related files of importance. These files can be cross referenced with other videos of similar visual content or associations for further analysis to establish connections between devices, individuals, or organizations. TREX is a scalable solution that can run on a laptop, cluster of machines, or in the cloud, and is currently serving various government agencies.

ONGOING PROJECT

Global Multilingual Social Media Analytics



The Global Multilingual Social Media Analytics tool provides translation and analysis of social media content and other publicly available information (PAI). It allows the user to understand what individuals, groups, and entire populations are discussing on common social media platforms which provides insight into how opinions are shifting in near real time and any developing actions as they occur. The project combined experiences and expertise across industries: Gantz-Mountain Intelligence Automation Systems enhanced their capabilities for exploiting and analyzing multilingual social media content; subcontractor SDL Federal Solutions, Inc. developed new statistical machine translation engines to provide translation of social media style content in Arabizi, Arabic dialects, Russian, Farsi, and Sahel French; and subcontractor Raytheon BBN integrated new features into the Multimedia Monitoring System (M3S) to support these operationally relevant languages and develop support for VKontakte, an important social media platform used throughout Eastern Europe. Raytheon BBN also enhanced the social media analytic capabilities in M3S based on specific user requirements, increasing M3S interoperability with other analytic platforms by developing data interchange formats.

MEMBERSHIP

Intelligence Community

Special Operations Forces

U.S. Department of Homeland Security

- Homeland Security Investigations

U.S. Department of Justice

- Federal Bureau of Investigation

TACTICAL OPERATONS SUPPORT

tossubgroup@cttso.gov

FOCUS AREAS

Offensive Systems

Develop advanced equipment and capabilities that enhance the effectiveness of small tactical units engaged in direct action operations. Develop specialized weapons, munitions, detonators, distraction/diversion devices, and other unique tactical equipment.

Unconventional Warfare and Counter-Insurgency Support

Develop advanced tools and equipment specifically for small tactical units conducting a broad spectrum of military, paramilitary, special warfare, and digital operations focused on force protection, assisted and unassisted recovery, and operational preparation of the environment.

Tactical Communications

Develop flexible, enhanced, full spectrum communications capabilities specifically designed for tactical forces, with emphasis on reducing operational load while improving operator mobility and efficiency. Develop assured tactical communications connectivity in challenging environments such as complex urban, subterranean, and maritime.

Tactical Reconnaissance, Surveillance, and Target Acquisition Systems

Develop technologies to assist small tactical teams in conducting organic reconnaissance, surveillance, and target acquisition missions. Develop systems that enhance the visual perception or other imaging capabilities of tactical operators in all conditions and environments.

Specialized Infiltration, Access, and Exfiltration Systems

Develop technologies that assist tactical assault forces in gaining rapid insertion, access and egress to, on, and from objectives. Improve evaluation of tactical options, and support efficiency and stealth, including remote operations. Develop enhanced target analysis, manual and dynamic breaching technologies for small tactical assault teams.

Survivability Systems

Develop man portable tools and equipment to enhance operator survivability during the conduct of tactical missions.

COMPLETED PROJECTS

5.56 mm Polymer Ammunition

While current brass-cased small arms ammunition is reliable, it adds considerable weight to already overloaded tactical operators. Polymer materials and cartridge case technologies have advanced to a state of maturity that allows modern lightweight polymers to be used in the construction of hybrid 5.56 mm cartridges that weigh 27 percent less than legacy brass-cased cartridges. This reduces the weight of the standard ammunition combat load of an M249 Squad Automatic Weapon (SAW) gunner from 20 to 14 pounds and that of a rifleman from 5.6 to 3.9 pounds. This bilateral effort with the United Kingdom challenged industry to develop and deliver polymer-cased ammunition that functions like legacy metallic-cased equivalents in unmodified, in-service carbines and belt-fed light machine guns in extreme environments. Phase I deliverables met both threshold and objective weight reduction goals and passed extreme temperature testing from -65°F to 165°F. Fifty-thousand 5.56 mm polymer rounds developed by MAC, LLC were evaluated in the United Kingdom with U.S. Government and U.S. Army small arms stakeholders. This revolutionary lightweight cartridge technology is being used to develop additional calibers and special applications in support of urgent tactical requirements.

Lightweight Intermediate Caliber Cartridges (LICCs)

The Lightweight Intermediate Caliber Cartridges (LICC) requirement challenged industry to develop lightweight conventional-configuration combat cartridges that would operate in traditional carbines, rifles, and belt-fed machine guns while also providing "overmatch" over the enemy through an extended maximum effective range (+300 meters) and terminal effects on targets beyond current U.S., NATO, and threat weapon capabilities. Using United States Joint Service, Canadian, and United Kingdom performance specifications compiled during two caliber workshops hosted by CTTSO, the U.S. Army Marksmanship Unit developed two intermediate caliber cartridges in both 6.5 mm (.264") and 7 mm (.277") calibers that were chosen for the LICC project.

The selected industry developer, MAC, LLC, provided technical solutions that reduced the weight of the "264 USA" and "277 USA" LICC rounds by 28 percent. Phase II deliverables included 2,500 rounds of both calibers in three assorted loads that were evaluated to generate data to support and inform ongoing United Kingdom and Canadian caliber studies, the U.S. Army Small Arms Ammunition Configuration (SAAC) Study, and United States Special Operations Command's (USSOCOM) Intermediate Caliber initiatives. These studies are focused on informing the optimum squad common caliber and cartridge requirements for the next generation of small unit weapon systems for Army and SOF warfighter use in 2020 and beyond. U.S. DoD, interagency, and United Kingdom and Canadian operational evaluations will be conducted through FY17.

Next Generation Small Arms Signature Reduction

The next generation suppressor for the MK18 Close Quarters Battle Rifle (CQBR) and M4 carbine is designed to reduce audible, visual, and thermal signatures. This newly developed suppressor, produced by Operator Suppressor Systems, features a forward flowing design that is intended to remedy problems and shortfalls found in fielded gas capture systems. Specifically, the new suppressor design decreases both bolt carrier speeds and backpressure which can contribute to malfunctions. Furthermore, the suppressor's forward flow design reduces excess weapon fouling and health concerns for the operator from toxic blowback. U.S. DoD, interagency, and United Kingdom operational evaluations will be conducted through FY17.

Military Free-Fall Tactical Tool (MFF-T2)

Tactical operators conducting military free-fall (MFF) parachute operations required an improved and advanced compact, modular navigation board that uses digital and analog technology for optimal situational awareness, ability to navigate accurately in all conditions, and the ability to standardize free-fall training and operations. MFF-T2 provides the ability for the operator to customize their individual and team jump boards, allowing each MFF parachutist the ability to quickly view and operate their GPS, compass and other navigation tools during High-Altitude High-Opening (HAHO) MFF operations. The MFF-T2 is a durable anti-shock kit that is also resistant to warping, corrosion, UV light and general defects resulting from common contaminants and corrosives. The MFF-T2 consists of an Android based situational awareness tool (ATAK) capable of full motion video viewing, Blue Force Tracking, telestration, and person-to-person chat; thus, enhancing tracking and MFF teams' ability to communicate and group while under canopy. Components and instruments of the MFF-T2 emphasize accurate navigation for all parachutists during HAHO or High-Altitude Low-Opening (HALO) operations

in non-permissive environments when accountability of all personnel, equipment, and accurate navigation is critical to mission success. Over fifty kits were provided by industry partners ADI Technologies, Inc. and Juggernaut Defense, LLC to Department of Defense and interagency tactical units for operational evaluation through FY16.

Underwater Vision Enhancement (UVE)

The Underwater Vision Enhancement (UVE) device allows Explosive Ordinance Disposal (EOD) divers the ability to work hands-free and perform render-safe procedures, as well as close quarter prosecution of ship attack charges and water-borne improvised explosive devices (WBIEDs) at night or in reduced visibility. The UVE device interfaces with the current standard Navy Mk20 dive mask, allowing the diver the ability to conduct hull/maritime structure search and inspection in both clear and turbid water without the use of an external light source while also enhancing vision above the water line. The UVE uses a combination of cutting edge sensor, display, and software technologies to provide the first all-digital, true color, and dive ready night vision device that gives the diver a large field of view at a higher resolution. DoD, interagency, and UK EOD dive units received final production kits by industry partner AMP Research, Inc. for maritime operational evaluation through FY17.

ONGOING PROJECTS

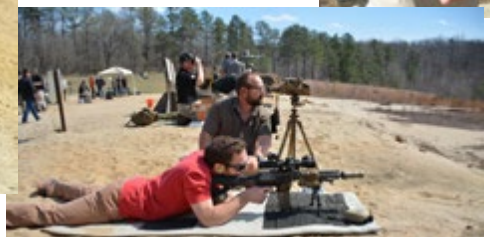
Ammunition Initiatives Meeting (AIM) Workshop and Advanced Technologies Live-Fire Demonstration

The individual tactical operator armed with small arms and ammunition is the most employed weapon system in the fight against terrorism in U.S. and allied arsenals. The AIM Workshop is a three-day Department of Defense,

interagency, and select international partner subject matter expert workshop created, organized, and conducted by the Tactical Operations Support Subgroup in response to user community requests to bring together both government and select industry representatives. The AIM Workshop is attended by more than 60 agencies from the United States, Australia, Canada, and the United Kingdom. AIM also includes a live-fire demonstration of advanced technologies from both government and industry developers. AIM discusses new and promising initiatives related to small caliber ammunition (to include 40 mm) and related weapon and accessory development and use. The AIM Workshop meets annually with these primary focus areas in mind:

- Threat Weapon and Ammunition Developments
- Joint U.S. and International Lessons Learned/ Capability Gaps Session
- The Law Enforcement Prospective
- Government and Industry Domestic/ International Ammunition/Small Arms Initiatives
- Exterior and Wound Ballistics Overview and Testing
- Lightweight Ammunition and Intermediate Caliber Cartridge Technology Development
- Projectile Aerodynamic Design, Interior/ Exterior Ballistics, and Terminal Effects
- Modern Ammunition Production and Testing
- Next Generation Ammunition, Projectile, Propellant, and Case Technology

In its eighth year in 2016, the AIM Workshop has been the incubator for rapid interagency development of various novel and advanced ammunition technologies to include lightweight polymer combat ammunition with enhanced terminal performance, intermediate caliber rifle and machine gun cartridges to improve standoff range for allied tactical personnel, advanced next generation sighting devices, and signature suppression as well as a vast assortment of new CT-related technologies.

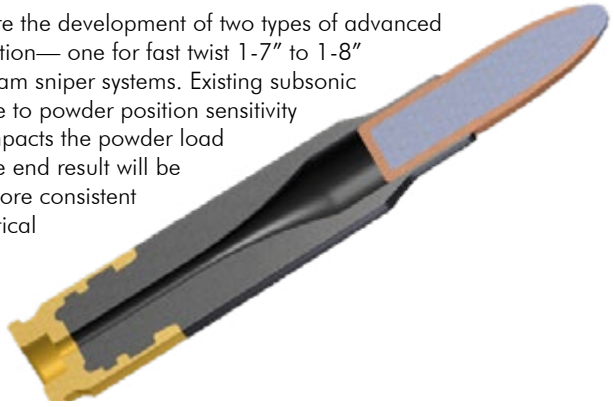


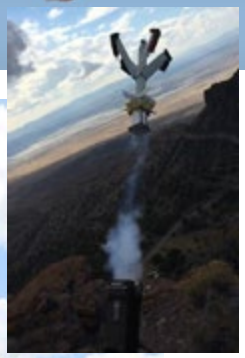
.338 Norma Magnum Lightweight Medium Machine Gun (LWMMG) and Polymer Cartridge

United States and United Kingdom tactical operators seek to develop the first of its kind .338 Norma Magnum (NM) polymer-cased cartridge that will advance the current capabilities of the Lightweight Medium Machine Gun (LWMMG) developed by industry partner General Dynamics Ordnance and Tactical Systems. Tactical operators currently use .50 caliber M2HB/M2A1 heavy machine gun for fixed site and mounted operations, weighing 82 pounds and having a max effective range of 2000 meters. The M240L 7.62 mm medium machine gun weighs 23 pounds and has a max effective range of 1000 meters primarily used for dismounted operations. The LWMMG, coupled with a polymer-cased .338 NM cartridge, will fill the capability gap between the ballistic capabilities of the M240L 7.62 mm medium machine gun and the .50 caliber M2HB/M2A1 heavy machine gun. The superior ballistics of the .338 NM offers improved accuracy, extending the direct fire effective range of a medium machine gun to 2000 meters. The current .338NM LWMMG weighs 23 pounds. CTTSO is developing a .338 NM polymer-cartridge that is projected to weigh 30 percent less than conventional brass cartridges. The polymer-cased cartridge will provide the same or better survivability in extreme temperatures, increase the longevity of the gun and allow for greater projectile mass for additional payload options (e.g., armor piercing, multipurpose and Saboted light armor penetrator). Reducing small tactical teams' organic equipment load and introducing a lighter agile weapon system coupled with the polymer-cased cartridge will maximize their ability to emplace this capability on a variety of ground, maritime, and aviation platforms and quickly transition to dismounted operations. Upon the completion of the development of .338 NM polymer-cased cartridge in FY17, tactical operators will perform live-fire testing in both the United States and the United Kingdom.

7.62x51 mm NATO Subsonic Ammunition Optimization - Position Insensitive Subsonic Round (PISR)

United States and United Kingdom tactical operators require the development of two types of advanced rounds for precision subsonic 7.62x51 mm NATO ammunition— one for fast twist 1-7" to 1-8" twist sniper systems and one for 1-10" to 1-12" twist program sniper systems. Existing subsonic sniper rounds do not provide the required performance due to powder position sensitivity issues. Through a new and advanced case design that compacts the powder load and ensures consistent ignition and burn characteristics, the end result will be an optimized subsonic round that has greater range and more consistent accuracy which will greatly improve the effectiveness of tactical operators in situations that require subsonic ammunition.





HERO-30SF Lethal Miniature Aerial Munition System (LMAMS)

Small tactical teams require a surgical strike, organic capability for operations in areas when fire support assets are limited or not available. The HERO-30SF Lethal Miniature Aerial Munition Systems (LMAMS) is being developed to provide increased lethality, deeper attack angles, increased loiter time, and an advanced training simulator capability. The goal of the project is to increase first-round hit capabilities in urban environments and challenging terrain. The HERO-30SF LMAMS is stored, carried, and can be launched from its portable canister and go directly to the intended target, or conduct intelligence, surveillance, and reconnaissance (ISR) until the enemy is confirmed, allowing the operator to find, fix, and finish a target of opportunity. The capability allows engagement of enemy combatants without exposing the tactical operator to direct enemy fires, allowing time sensitive engagement of line-of-sight (LOS) or beyond line-of-sight (BLOS) stationary or moving targets. The HERO30-SF is being developed by Mistral Inc. leveraging existing warhead and fuze designs developed by the U.S. Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC). Flight testing will be conducted at the U.S. Army Dugway Proving Ground. Military tactical operators will receive complete kits in FY17 for operational test and evaluation.

Cyber Operator Greyhat (COG)

The digital domain will be key terrain on future battlefields. The United States and its allies continue to encounter an increasing cyber threat where a "Digital Divide" exists between the U.S. and our cyber opponents. Government and military organizations are standing up capacities and capabilities to address this threat at the strategic level. At the request of Special Operations Forces (SOF), CTTSO took the initiative to complement this larger build by training operators at the tactical level. Cyber Operator Greyhat (COG) is an unclassified, open-source digital operations course tailored to train tactical operators to understand the cyber domain and to identify and mitigate cyber threats. The five-week intensive courses provides foundations in computer science, information security, social media, and advanced computer networking. The classroom instruction was validated with practical field training events and one comprehensive full mission profile, three-day culmination exercise designed to build organic capacity to protect the network, and detect and correct an intrusion using best practice digital operations methodologies. COG contributed to the development of SOF tactical capabilities to enable digital operations. The

COG course, conducted by industry partners Advanced Mission Systems and SensePost, trained over 120 SOF, U.S. DoD, interagency, and select international partner operators from FY15 through FY17. The Program of Instruction (POI) and Mission Essential Task List (METL) from the COG course are transitioning to United States Army Special Operations Command in FY17.

Cyberspace Open Source Methods and Operations (COSMO)

Protection against current digital threats requires special skills in order to understand and operate in the digital battle space. The 21st century social media medium is being leveraged and exploited by both state and non-state actors to recruit, command, control, and conduct illegal and terrorist activities against the United States and allied interests. COSMO is a three-week intensive, tactical level training course that teaches operationally relevant capabilities to execute digital force protection and operational security for publicly available information. The course introduces state-of-the-art social media tools and applies them to operationally relevant themes. COSMO students are taught to find, gather, and analyze online data and metadata via a hybrid process of iterative search, discovery, and analysis. Students return to their tactical units exceptionally trained to organically operate effectively and safely in the digital domain. By design, COSMO is a unique, combined, joint, interagency digital task force training environment that has trained over 140 SOF, U.S. DoD, interagency, and select international partner operators from FY15 through FY17 by industry partner White Canvas Group.

GreenZone Secure Communications Suite

Tactical operators require secure and discreet communications for operations. The GreenZone Secure Communications Suite (GSCS) endeavors to meet the priority communications needs of tactical operators by creating a secure ecosystem based on a holistic communications approach of combining cutting edge software, hardware, and telecommunications technologies. This capability features a public key infrastructure (PKI) based software suite for versatility on common operating systems; a virtual machine based routing system for infrastructure connectivity for data in transit (DIT) and data at rest (DAR) security solution. GSCS brings tactical communications into the 21st century by allowing the use of smartphone devices and technologies off of the Department of Defense Information Network (DoDIN) through an approved for use (Risk Management Framework / Authority to Operate) solution architecture that allows for plug-n-play flexibility with third party applications and hardware. Military and interagency tactical units conducted test and evaluation in FY16 and are projected to conduct additional testing on spiral developed kits in FY17 that integrates with the government-off-the-shelf (GOTS) Android Tactical Assault Kit (ATAK).

Silicon Membrane Amplified Lightweight Speaker (SMALS)

The Silicone Membrane Amplified Lightweight Speaker (SMALS) project is developing a state-of-the-art amplified speaker-transceiver unit to work with a number of military and commercial primary radio devices. SMALS leverages current technologies and integrates them to provide an advanced system that enhances current communications packages.

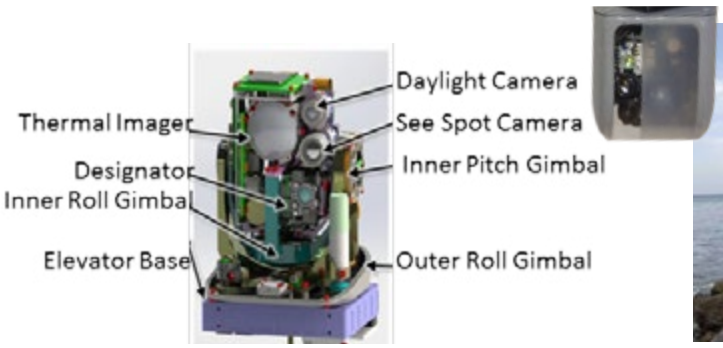
The SMALS provides extended frequency response, along with vastly improved audio output. GromaTech's development has coupled high performance audio drivers with a specially tuned acoustic chamber resulting in superior performance for today's war fighters at one-fifth the weight and less than half the size of the currently fielded radio speaker. Units are receiving additional prototypes in FY17 for operational test and evaluation.

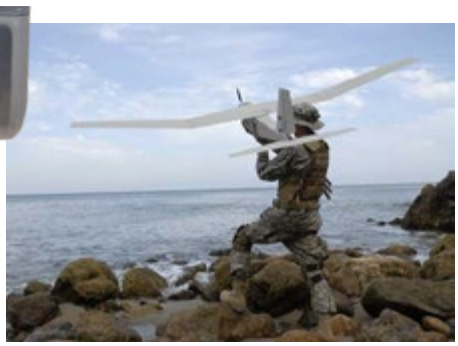
Maritime Canister Launched Small Unmanned Aircraft System (MCLSUAS)

Small tactical teams operating in maritime environments require an organic small unmanned aircraft system (sUAS) capable of being deployed and controlled while submerged to support surface surveillance and reconnaissance missions. The MCLSUAS, being developed by Lockheed Martin's Mission Simulations and Training Division, provides maritime forces the capability to launch a collapsible-wing sUAS in sea state three conditions, while also allowing recovery and reuse on land or sea. The MCLSUAS features: Vector Hawk sUAS; Canister Launch Unit; Maritime Ground Control Station. The Vector Hawk sUAS has a minimum operating time of 70 minutes, 50 knots dash speed, 15 to 20 knots stall, and will stay afloat for a minimum of 30 minutes for recovery and reuse after water landing. Four systems are scheduled for delivery, training, and operational evaluation in FY17.

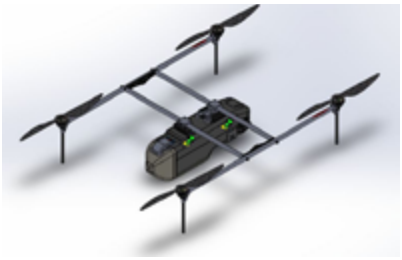
Miniature Gimbal Laser Target Designator Payload for Small Unmanned Aircraft System (sUAS)

This project provides the PUMA sUAS with a next-generation stabilized and gimballed payload that combines long wave infrared (LWIR) technology, a laser target designator, and a see-spot capability for positive identification of the laser spot on target. When fielded, tactical operators will have the organic capability to immediately transition from surveillance to targeting operations using the same payload. CONTROP USA, Inc. and Avwatch, Inc. are providing two payloads for test, evaluation, and final delivery in the second quarter of FY17.

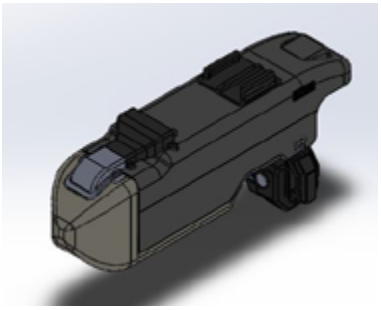




Multi-Ability Reconfigurable Small Unmanned Aircraft System (MARSUAS)

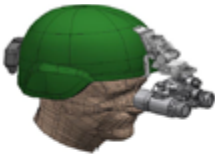


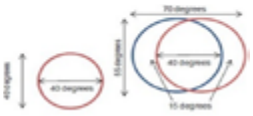
Tactical forces currently operate single form factor Group 1 Fixed and Vertical Lift sUAS to perform current mission tasks. Units are challenged with maintaining currency, training standardization, interoperability on multiple platforms, sustainment of the systems, and an increase in operational load when deploying these different sUAS. The MARSUAS project will provide operators with a single sUAS platform that can be configured in the field to support missions requiring a quad rotor sUAS, tilt rotor/vertical takeoff and lift sUAS, and fixed wing long endurance sUAS with one common tablet controller. When fielded, operators will have a rapidly reconfigurable sUAS that has the potential to replace all existing Group 1 sUAS. UAV Solutions, Inc. is providing four systems for training and testing in the fourth quarter of FY17.

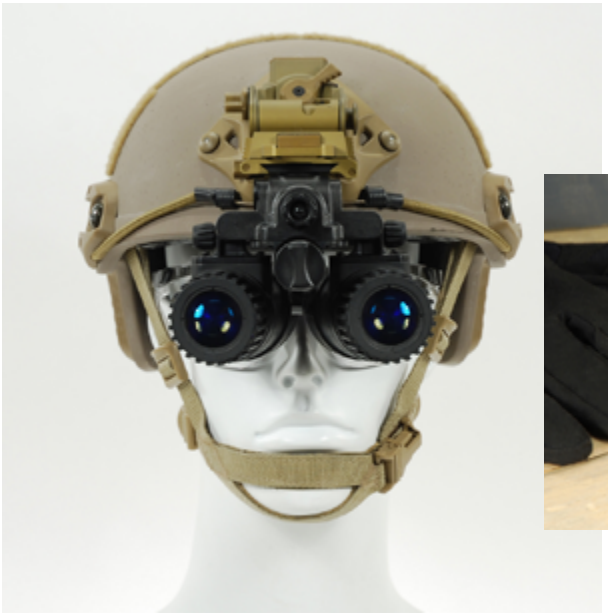


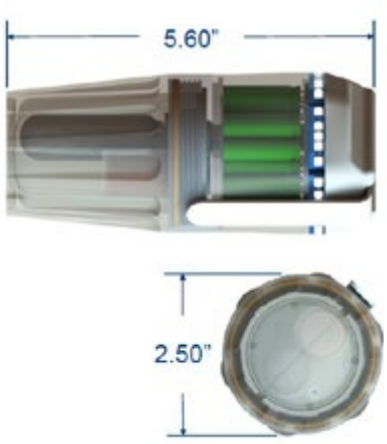
Wide Field of View Binocular Night Vision Device (WFOV BNVD)

The WFOV BNVD is being developed to provide tactical operators an advanced capability that increases the field of view to 70 degrees horizontal and 50 degrees vertical, and also improves the figure of merit of the tubes at an affordable price. L-3 Communications will provide six WFOV BNVDs in FY17 for operational test and evaluation by DoD tactical operators.









Non-Pyrotechnic Diversionary Device (NPDD)

Current noise/flash diversionary devices (NFDD) rely on a small quantity of pyrotechnic material to create a loud noise and brilliant flash that is intended to distract and disorient adversaries during tactical operations. These NFDDs create small shrapnel and sparks which may cause unintended injury, explosions, or fire when employed near flammable gases or materials. The NPDD, in development by Applied Research Associates, Inc., is a reloadable/reusable device that provides operators with an improved and advanced, intrinsically safe (non-pyrotechnic and non-toxic) means to distract and disorient adversaries in high-risk/high-threat hazardous environments where currently fielded standard pyrotechnic means may cause unintended collateral damage to non-combatant personnel and facilities. DoD, interagency, and UK tactical units will receive final production kits and new equipment training to conduct operational evaluations through FY17.

Augmented Reality System - Navigation (ARES-N)

Currently, tactical operators conduct route planning and navigation during missions using applications such as the Android Tactical Assault Kit (ATAK), which allows them to simultaneously view navigation directions/data and friendly and/or foe positions. However, there is no safe way to drive or navigate a vehicle while in a combat or hazardous area without one team member looking down at a mobile device running these current capabilities. The ARES-N project aims to have both the driver and all team members with their heads up for force protection during mobile operations through a dashboard mounted tablet and software based solution. ARES-N, developed by industry partner PAR Government Systems Corporation, features an augmented reality system that overlays a tablet camera's live footage, navigation instructions, and targeting information. DoD and interagency tactical operators will conduct test and evaluation of the ARES-N kits in early FY18.

MEMBERSHIP

National Tactical Officers Association

State and Local Agencies

- Austin (TX) Fire Department
- Boston (MA) Special Weapons and Tactics
- Charleston (SC) Special Weapons and Tactics
- Denver (CO) Special Weapons and Tactics
- Indianapolis (IN) State Police Bomb Squad
- Los Angeles (CA) Police Department
- Los Angeles Sheriff's Department
- Maryland State Police Special Weapons and Tactics
- Massachusetts State Police Bomb Squad
- New Jersey State Police
- New York City Police Department and Fire Department
- Pasco County (FL) Sheriff's Office
- San Diego (CA) Sheriff's Department
- San Diego Fire Department and Bomb Squad
- Savannah (GA) Special Weapons and Tactics
- South Carolina State Police Bomb Squad
- South Carolina State Police Special Weapons and Tactics

U.S. Department of Defense

- Cyber Command
- Defense Intelligence Agency
- Joint Improvised-Threat Defeat Organization
- Joint Personnel Recovery Agency
- National Guard Bureau
- National Security Agency
- U.S. Air Force
  - Explosive Ordnance Disposal
- U.S. Army
  - 20th Support Command, CBRNE
  - Armament Research, Development, and Engineering Center
  - Asymmetric Warfare Group
  - Maneuver Center of Excellence
  - Night Vision and Electronic Sensors Directorate
  - Office of the Army G-3/5/7 (Operations/Plans)
  - Office of the Army G-8 (Financial Management)
  - Program Executive Office Soldier
  - Program Manager Unmanned Aircraft Systems (PMUAS)
  - Rapid Equipping Force
  - Soldier Systems Center
- U.S. Marine Corps
  - Explosive Ordnance Disposal
  - Marine Corps Forces Cyber Command
- U.S. Navy
  - Naval Academy
  - Naval Air Weapons Station, China Lake
  - Naval Postgraduate School
  - Naval Surface Warfare Center, Carderock Division
  - Naval Surface Warfare Center, Crane Division
  - Naval Surface Warfare Center, Dahlgren Division
  - Navy Explosive Ordnance Disposal Group 2
- U.S. Special Operations Command
  - Air Force Special Operations Command
  - Army Special Operations Command
    - 1st Special Forces Command (Airborne)
    - 75th Ranger Regiment
    - Army Special Operations Aviation Command
    - Civil Affairs
    - Military Information Support Operations Command
    - U.S. Army John F. Kennedy Special Warfare Center and School
  - Joint Special Operations Command
  - Marine Corps Forces Special Operations Command
  - Naval Special Warfare Command
    - Naval Special Warfare Groups
    - Special Boat Teams
  - Theater Special Operations Commands

U.S. Department of Energy

- National Nuclear Security Administration

U.S. Department of Homeland Security

- Customs and Border Protection
  - Border Patrol Tactical Unit
  - Border Search, Trauma, and Rescue
  - Special Operations Group
- Federal Air Marshal Service
- Immigration and Customs Enforcement
  - Homeland Security Investigations
- Office for Bombing Prevention
- Transportation Security Laboratory
- U.S. Coast Guard
  - Maritime Security Response Team
  - Maritime Safety and Security Team
- U.S. Secret Service

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
  - Special Response Teams
- Drug Enforcement Administration
  - Special Operations Division
- Federal Bureau of Investigation
  - Ballistic Research Facility
  - Critical Incident Response Group
  - Hostage Rescue Team
  - Washington Field Office
- U.S. Marshals Service

U.S. Department of State

- Bureau of Diplomatic Security

TRAINING TECHNOLOGY DEVELOPMENT

ttdsubgroup@cttso.gov

FOCUS AREAS

Innovative Training and Educational Concepts

Research, develop, and evaluate training and educational programs that employ novel instructional design and/or delivery methods for accelerating and enhancing the acquisition of advanced knowledge and skills.

Human Performance Technology

Analyze the full range of performance gaps and select interventions to improve and sustain human performance. Develop, test, and evaluate performance improvement technologies and programs based on cognitive and physiological principles to optimize operator training and ultimately mission performance.

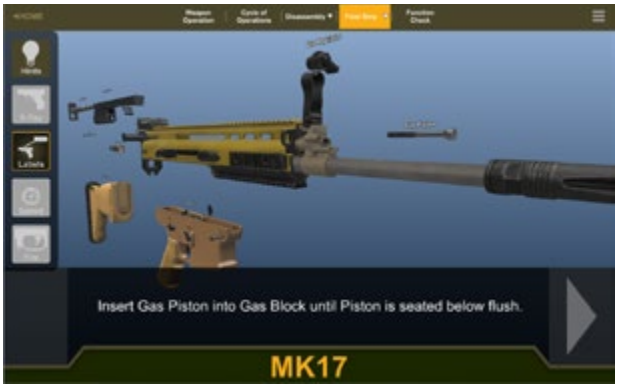
Mobile Learning

Design and develop intuitive, interactive learning solutions for anywhere, anytime access from mobile devices. Develop mobile applications and technology that supports learning through ubiquitous and just-in-time access to educational resources, collaborative learning environments, and user-generated content.

Immersive Learning Technology

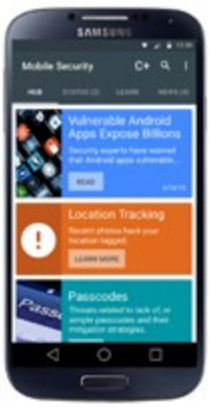
Research and develop technology that allows a learner to seamlessly interact with, and become immersed in, a learning environment. Develop tools, technologies, and techniques for improving the design, development, and validation of interactive and immersive learning technology.

COMPLETED PROJECTS



3D Weapons Models and Mobile Application

Under current armorer weapons training, the ability to observe the functions of weapon system parts during live fire is non-existent. Students are limited in terms of the amount of interaction they can have with certain weapons while in class, at home, or in the field. While students can be informed of commonly experienced weapon malfunctions, a thorough understanding of the interaction of internal parts during the cycles of operation assists greatly in troubleshooting and repairing. This was an effort to design and develop interactive weapons 3D software that allows students to study and practice newly acquired skills away from the classroom environment, increasing proficiency and greatly enhancing the formal instruction. The application, featuring 21 weapon models, allows end users to see the inner workings of the weapons and manipulate those weapons in 3D, as well as to practice assembly, disassembly, and function checks on each weapon. The 3D Weapons application is available as a standalone Windows desktop application, and on Android and iOS devices for download through CTTSO and the U.S. Army Training and Doctrine Command (TRADOC) Application Gateway.



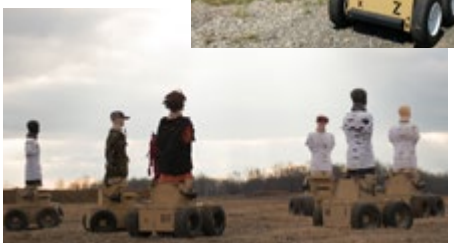
Mobile Security in Operational Environments

Mobile security news and practices are ever changing due to identification of new vulnerabilities and nearly constant updates to operating systems. Float Mobile Learning designed and developed an innovative and unique custom mobile training and performance support application for iOS and Android devices that provides up-to-date information on security news and turns the device itself into a powerful security assessment tool. The app provides mobile security education and device assessment tools to assist operators in using their devices more safely. Current security news, tips and tricks, and a diagnostic toolset to determine current threats present on the device are combined to create a useful app for operational personnel. The app is available for download and can be obtained by contacting the Training Technology Development Subgroup.

ONGOING PROJECTS

Virtual Reality Part Task Trainer (vrPTT)

The Air Force Special Operations Command's (AFSOC) part task trainers are immobile and often unavailable for continued pre- and post-operations training. The AC-130U vrPTT project is aimed at overcoming this limitation by developing an AC-130U part task training capability consisting of an interactive 3D high-definition virtual reality environment integrated with an automated and interactive intelligent virtual instructional tutor. The vrPTT end product will consist of an untethered, wearable, and lightweight visual display linked to a high capacity computer. Users will be able to view, manipulate, and operate 3D high-definition virtual images of aircraft mission systems and components through "bare-handed" interactive functions to provide real time feedback (i.e., touch, move, operate, and access selectable exploded views of components). The automated and interactive intelligent tutoring program will mimic the Visual Threat Recognition and Avoidance Trainer instruction and learning methodology, will adjust in complexity and progression based on graduated skill development, and will include task performance evaluation and remediation. Two fully functional vrPTT systems will be delivered to AFSOC at the end of the contract and an extension to other aircraft and Commands is under consideration.



Low-Cost Robotic Human Type Targets

Due to training environment and resource constraints, live fire on a realistic moving target is often experienced for the first time during combat or other hostile situations instead of during training exercises. The Low-Cost Robotic Human Type Target system, being developed by Marathon Targets, addresses this training challenge by providing operators with realistic targets at a price that promotes accessibility to more military and law enforcement end users. Marathon Target's existing T40 target is an autonomous trackless target which was primarily designed for Special Forces who are in need of reality-based training with unpredictable scenarios as well as training of dynamic tactical maneuvers. The low-cost version of the existing T40 target has been designed based on a needs analysis and feedback from various end user groups who have previously used the T40 target system during live-fire exercises. Two major use cases have been identified for which the new target model will be specialized: a) moving marksmanship training (infantry and sniper), and b) combined-arms exercises. This will result in more effective training for military and law enforcement personnel translating into optimal performance when encountering threats in the operational environment. Four final target systems will be delivered to the government and additional low-cost versions will be available for purchase.

Maritime Low Observable Identification Capability

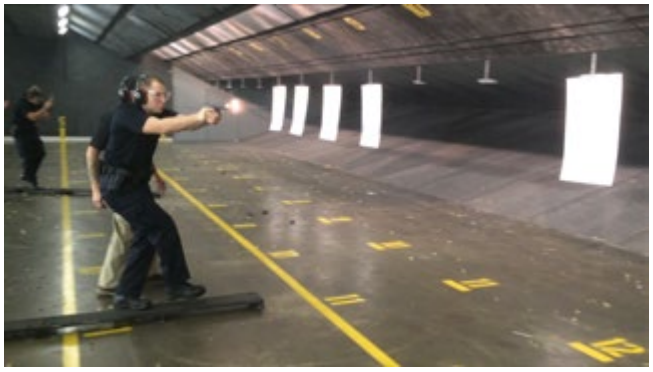
The Maritime Low Observable Identification Capability (M-LOIC) program is an effort to design, develop, and implement maritime surveillance training and technology solutions to identify and defeat combatant networks operating in and around the maritime environment that pose a continued transnational threat to the United States and partner nation forces abroad. The program commenced with detailed research and analysis to properly identify existing training and technology capability gaps to support maritime surveillance operations. To address the identified gaps, an iterative design process was used to develop multiple training courses that end users attended to properly evaluate each topic of instruction. The iterative design process supports building a comprehensive program of instruction for future integration into pre-deployment training cycles. Similarly, program efforts are dedicated to developing technology solutions to support low visibility operations on non-standard surface maritime mobility platforms. All research conducted throughout the program is ongoing to ensure continued operational relevance for the end user community in both training and technology supporting real-world operations. The program will be integrated into the end user's current training cycle for long-term sustainment beyond the contract.

Task Force Officer Mobile Learning and Performance Support

Task Force Officers (TFOs) have increasingly complicated jobs and ever-increasing bodies of knowledge that they must pull from in order to execute their work effectively. As this demand increases, the rules, regulations, and role-specific considerations are also becoming more difficult to navigate. Currently, Homeland Security Investigations offers a 40-hour instructor-led training course and refresher training that are offered occasionally. Limited funding and personnel availability, however, has reduced course completion leading to far fewer TFOs than needed. Float Mobile Learning is designing and developing a distance learning application to augment the instructor-led

course that will allow a sufficient number of TFOs to perform their duties alongside their Federal Law Enforcement partners. Float Mobile Learning is developing the solution and tools to be accessible for smartphones and tablets running iOS and Android OS, with Windows Mobile and Desktop Web Browser as optional additional platforms. A wide range of learning tools from courseware and media delivery to performance support and just-in-time information delivery is being created. The application will provide TFOs new ways to access training material and information as needed to overcome existing resource constraints and facilitate greater personnel readiness.

Operational Motor Skills and Reactionary Engagements Training



The purpose of this bilateral effort with Canada is to evaluate a training capability that addresses the gap between basic firearms training and more advanced tactical and dynamic shooting techniques for law enforcement agencies within the United States and Canada. Traditional law enforcement firearms training is often conducted under sterile conditions with known factors, controlled environments, and precise qualification requirements. Recent events and emerging threats, however, have demonstrated the need for more realistic training with stress factors including time, proximity/distance, grip, stance/movement, and scenarios similar to an active shooter engagement. An existing five-day United States Pentagon Force Protection Agency (PFPA) 'Reactive Shooter Operator' course will serve as the foundation for this effort. The course focuses on performing in various environments, under high-stress situations, while maintaining proper grip/control and shooting with accuracy. The course will be modified to gather baseline physiological data for comparison of various stress factors and instructional techniques such as incorporating training simulation technology. Physiological data will be collected through the use of wearable recording technology that will be worn by participants throughout the duration of the course. The course evaluation results will be compiled and shared with the defense departments of the United States and Canada, and law enforcement organizations.

Tools and Techniques to Optimize Human Cognitive Performance

There are a number of commercially available tools and published techniques being used by the United States and United Kingdom special operations communities with the intent of optimizing cognitive performance. There is mixed evidence, however, to support claims that these tools and techniques actually optimize cognitive performance and that performance gains can transfer between the application and the real world. This bilateral task plan aims to address this gap and ensure that operators are provided with unbiased scientific evidence regarding cognitive performance tools and techniques. Initially, a literature review will be conducted to establish the scientific support for or against the use of such tools and techniques to improve performance on operationally relevant tasks among healthy adults. A spreadsheet will be compiled summarizing the research findings for operators to quickly identify the most beneficial tools for their training and performance improvement needs. The tools and techniques that appear to be most relevant for special operations training and performance improvement needs will be selected for further empirical study. The research findings will be made available to the United States and United Kingdom special operations communities.

MEMBERSHIP

Intelligence Community

InterAgency Board

National Bomb Squad Commanders Advisory Board

National Tactical Officers Association

U.S. Department of Defense

- Advanced Distributed Learning Initiative
- Defense Intelligence Agency
- Joint Improvised-Threat Defeat Organization
- Office of the Under Secretary of Defense for Personnel and Readiness
- Pentagon Force Protection Agency
- U.S. Army Asymmetric Warfare Group
- U.S. Marine Corps
  - U.S. Marine Training and Education Command
  - Weapons Training Battalion
- U.S. Special Operations Command
  - Air Force Special Operations Command
  - Army Special Operations Command
    - 75th Ranger Regiment
    - U.S. Army John F. Kennedy Special Warfare Center and School
  - Naval Special Warfare Command

U.S. Department of Homeland Security

- Customs and Border Protection
- Federal Law Enforcement Training Center
- Immigration and Customs Enforcement
  - Homeland Security Investigations
- Protection and Programs Directorate
  - Office for Bombing Prevention
  - Science and Technology Directorate
  - Transportation Security Administration
  - U.S. Coast Guard
  - U.S. Secret Service

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Bureau of Investigation
- Office of the Attorney General
- U.S. Marshals Service

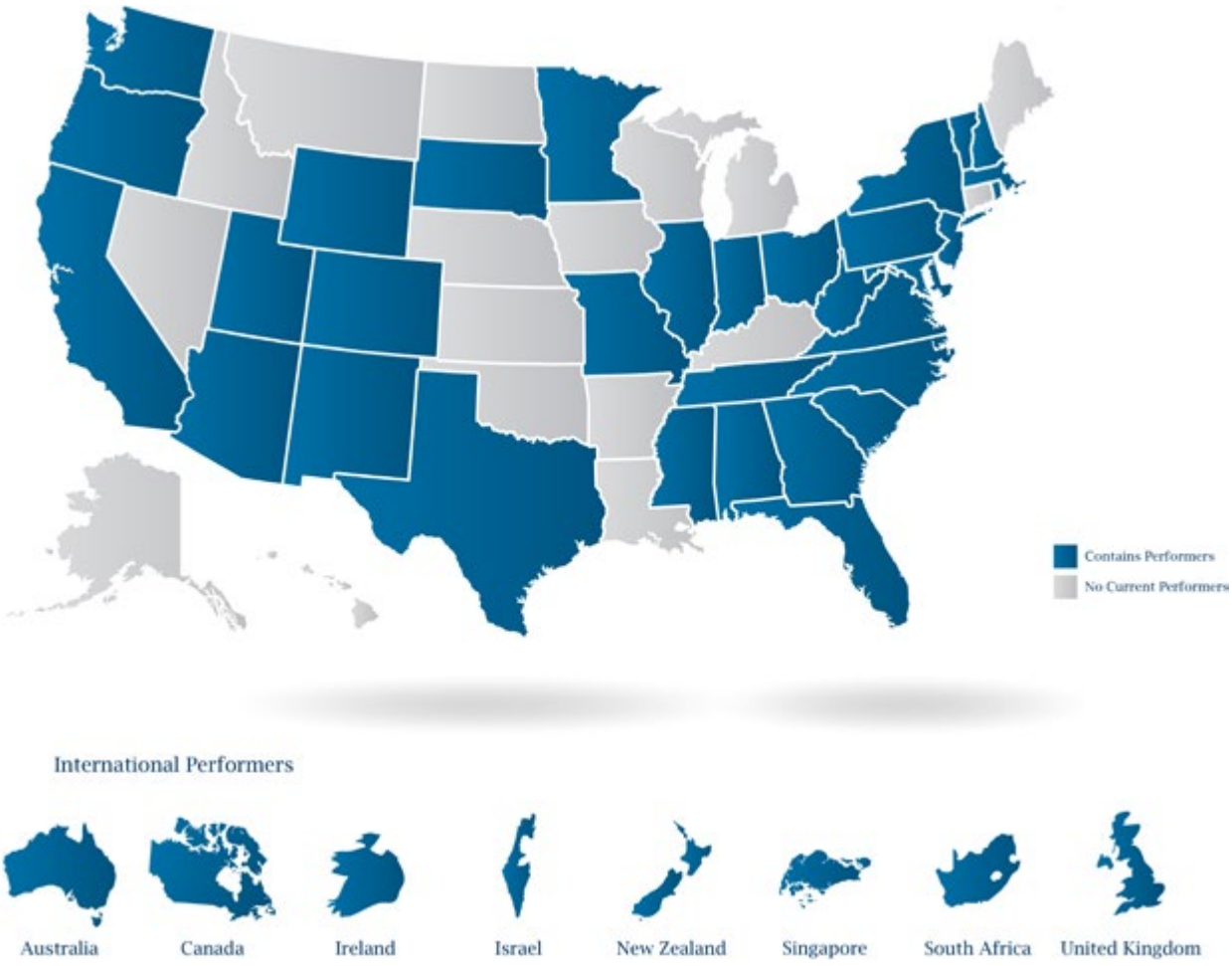
U.S. Department of State

- Bureau of Counterterrorism and Countering Violent Extremism
- Bureau of Diplomatic Security

U.S. Department of the Treasury

- Financial Crimes Enforcement Network

2016 PERFORMERS



Alabama

Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC), Redstone Arsenal

Kailos Genetics, Inc., Huntsville

Norshield Security Products, LLC, Montgomery

Arizona

Arizona State University, Phoenix

Impact Research and Technology, LLC, Phoenix

Juggernaut Defense, LLC, Scottsdale

Metris, LLC, Mesa

SAIFE, Inc., Tempe

California

AeroVironment, Inc., Simi Valley

Baker Engineering and Risk Consultants, Inc., El Segundo

Creative Radicals, LLC, Santa Rosa

Cubic Applications, Inc., San Diego

Decision Sciences International Corporation, Poway

EdVenture Partners, Orinda

Gantz-Mountain Intelligence Automation Systems, Inc., Carmel Valley

Kalloc Studios, Carlsbad

Lawrence Livermore National Laboratory, Livermore

Naval Health Research Center, San Diego

Naval Postgraduate School, Monterey

Naval Surface Warfare Center Crane Division, Fallbrook

Physical Optics Corporation, Torrance

RAND Corporation, Santa Monica

Rapiscan Systems, Sunnyvale

Seacoast Science, Inc., Carlsbad

Sonitus Technologies, Inc., San Mateo

Spectral Labs, Inc., San Diego

SRI International, Menlo Park

Tek84 Engineering Group, San Diego

Xone Technology, Inc., Santa Clara

XRSciences, LLC, Carlsbad

Colorado

Applied Research Associates, Inc., Littleton

NEK Advanced Securities Group, Inc., Colorado Springs

PathAR, LLC, Colorado Springs

RadiantBlue Technologies, Inc., Colorado Springs

Delaware

ILC Dover, Frederica

District of Columbia

Argent PLLC

Barbaricum, LLC

Department of Homeland Security Science and Technology Directorate

First Mile Geo

Naval Research Laboratory

Neptune

U.S. Institute of Peace

Florida

AMP Research, Inc., Naples

Florida International University, Miami

Harris Corporation, Melbourne

Naval Surface Warfare Center, Panama City

Navy Experimental Diving Unit, Panama City

Ocean Optics, Inc., Dunedin

RINI Technologies, Inc., Oviedo

Sc2 Corp, Clearwater

Studio 14b, LLC, Safety Harbor

Titus Human Performance Solutions, LLC, Tallahassee

Georgia

Georgia Tech Research Institute, Atlanta

Illinois

Argonne National Laboratory, Argonne

Float Mobile Learning, Morton

Motorola Solutions, Inc., Schaumburg

Vertex Solutions Group, Urbana

Indiana

Naval Surface Warfare Center, Crane

Purdue University, West Lafayette

Maryland

Army Communications-Electronics Research, Development and Engineering Center (CERDEC) Intelligence and Information Warfare Directorate (I2WD), Aberdeen Proving Ground

Army Research Laboratory, Aberdeen Proving Ground

Army Research Laboratory, Human Research and Engineering Directorate, Adelphi

Army Tank Automotive Research Development and Engineering Center, Aberdeen Proving Ground

Avon Protection Systems, Inc., Belcamp

Axom Technologies, Inc., Annapolis Junction

CyberReliant Corporation, Annapolis

Edgewood Chemical Biological Center, Aberdeen Proving Ground

Efficio, Inc., Laurel

ELTA North America, Fulton

GromaTech, LLC, Laurel

HP White Laboratory, Inc., Street

Intelligent Automation, Inc., Rockville

Johns Hopkins University Applied Physics Laboratory, Laurel

National Biodefense Analysis and Countermeasures Center, Frederick

Naval Surface Warfare Center, Explosive Ordnance Disposal Technology Division, Indian Head

Mistral, Inc., Bethesda

Ordnance Holdings, Inc., Reisterstown

Roboteam North America, Gaithersburg

Sierra Nevada Corporation, Integrated Mission Systems, Hagerstown

UAV Solutions, Inc., Jessup

WinTec Arrowmaker, Inc., Fort Washington

W.L. Gore & Associates, Inc., Elkton

Massachusetts

908 Devices, Inc., Boston

American Science and Engineering, Inc., Billerica

Avwatch, Inc., Plymouth

Blauer Manufacturing Company, Boston

Charles River Analytics, Inc., Cambridge

Physical Sciences, Inc., Andover

Pixel Forensics, Inc., Burlington

Raytheon BBN Technologies, Cambridge

Minnesota

GreenZone Systems, Inc., Minneapolis

Mississippi

Applied Research Associates, Inc., Vicksburg

Army Engineer Research and Development Center, Vicksburg

Camgian Microsystems, Inc., Starkville

Kopis Mobile, LLC, Flowood

MAC, LLC, Bay Saint Louis

Open Technology Center of Excellence, Camp Shelby

Stark Aerospace, Inc., Columbus

Missouri

MRIGlobal, Kansas City

New Hampshire

Gentex Corporation, Manchester

HALO Maritime Defense Systems, Newton

Kollsman, Inc. / Elbit Systems of America, Merrimack

L-3 Communications Corporation – Warrior Systems Sector, Londonderry

Wilcox Industries Corporation, Newington

New Jersey

Battelle Memorial Institute, Egg Harbor

Signature Science, Egg Harbor

SRI International, Princeton

Transportation Security Laboratory, Egg Harbor

New Mexico

Applied Research Associates, Inc., Albuquerque

Energetic Materials Research and Testing Center, Socorro

National Assessment Group, Kirtland Air Force Base

Sandia National Laboratories, Albuquerque

New York

Air Force Research Laboratory, Rome

Cornell University, Ithaca

GE Global Research, Niskayuna

Intertek, Cortland

Lockheed Martin Mission Systems and Training, Owego

PAR Government Systems Corporation, Rome

Persistent Systems, LLC, New York

Saint Gobain, Niagara Falls

North Carolina

Advanced Mission Systems, Charlotte

Horizon Performance, LLC, Cary

North Carolina State University, Textile Protection and Comfort Center, Raleigh

Ohio

Battelle Memorial Institute, Columbus

Lion Apparel, Inc., Dayton

nVisti Tactical Innovation, Inc., Cleveland

Oregon

Thetus Corporation, Portland

Pennsylvania

Gentex Corporation, Simpson

Mitigation Technologies, Mercersburg

Pennsylvania State University, State College

Rhode Island

Naval Undersea Warfare Center, Newport

South Carolina

Department of Energy – Savannah River Operations Office, Aiken

Southeast Efficiency Improvement Associates, LLC, Graniteville

South Dakota

Black Hills Ammunition, Rapid City

Tennessee

eSpin Technologies, Inc., Chattanooga

Universal Strategy Group, Inc., Franklin

Texas

Accuracy 1st, Inc., Canadian

Atlas Wearables, Inc.

Baker Engineering and Risk Consultants, Inc., San Antonio

Energetic Materials and Products, Round Rock

International Personnel Protection, Inc., Austin

Laser Shot, Inc., Stafford

Praevius Group, Inc., Salado

Protection Engineering Consultants, LLC, Austin

Signature Science, LLC, Austin

Southwest Research Institute, San Antonio

Utah

Dugway Proving Group, Dugway

ID Scientific, Park City

Operators Suppressor Systems, Salt Lake City

Vermont

General Dynamics Ordnance and Tactical Systems, Burlington

Virginia

Adayana Government Group, Falls Church

ADI Technologies, Inc., McLean

Battelle Memorial Institute, Arlington

Bode Cellmark Forensics, Lorton

Booz Allen Hamilton, Inc., McLean

Caerus Associates, Arlington

CONTROP USA, Inc., Manassas

DecisionQ Corporation, Arlington

Digital Reasoning, Arlington

HumanGeo, Arlington

H2OBR, Virginia Beach

Ideal Innovations, Inc., Arlington

In-Q-Tel, Arlington

Information Systems Worldwide, Arlington

IST Research, Fredericksburg

KForce Government Solutions, Fairfax

ManTech International Corporation, Chantilly

Metis Solutions, LLC, Alexandria

Millennium Engineering and Integration Company, Arlington

Naval Special Warfare Development Group, Virginia Beach

Naval Surface Warfare Center, Carderock

Naval Surface Warfare Center, Dahlgren

NexGen Communications, LLC, Dulles

Night Vision and Electronic Sensors Directorate, Ft. Belvoir

Novetta, Inc., McLean

Novetta, Inc., Reston

Ntrepid Corporation, Herndon

Oceans Edge, Inc., Reston

Orbis Operations, McLean

Pacific Architects and Engineers, Arlington

Progeny Systems Corporation, Manassas

Raytheon Blackbird Technologies, Inc., Herndon

Resonate Learning Consultants, LLC, Reston

Roka Security, Herndon

S4Tech, Inc., Sterling

Safety Equipment Institute, McLean

SDL Federal Solutions, Inc., Herndon

Segue Technologies, Inc., Arlington

Shoulder 2 Shoulder, Inc., Bluemont

Silverback7, Inc., Woodbridge

Sphere of Influence, Inc., McLean

System of Systems Analytics, Inc., Fairfax

Systems Engineering Technologies Corporation (SyTech), Alexandria

TextOre, Inc., Fairfax

Threat Knowledge Group, LLC, McLean

VECTARE, Inc., Fairfax

Veris, LLC, Vienna

White Canvas Group, LLC, Alexandria

ZTI Solutions, LLC, Edinburg

Washington

Analytical Methods, Inc., Kirkland

Cascade Designs, Inc., Seattle

Pacific Northwest National Laboratory, Richland

West Virginia

Azimuth, Inc., Morgantown

West Virginia Army National Guard, Camp Dawson

West Virginia High Technology Consortium Foundation, Fairmont

Wyoming

Snowy Range Instruments, Laramie

Australia

Australian Nuclear Science and Technology Organisation, Lucas Heights, New South Wales

ChemCentre, Bentley, Western Australia

Department of the Prime Minister and Cabinet, Barton, Australian Capital Territory

Defence Science and Technology Group, Canberra, Australian Capital Territory

Defence Science and Technology Group, Edinburgh, South Australia

Defence Science and Technology Group, Fisherman's Bend, Melbourne, Victoria

Flinders University, Adelaide, South Australia

Ideation Product Solutions Pty. Ltd., Burwood, Victoria

Marathon Targets, Sydney, New South Wales

Queensland Fire and Emergency Services, Brisbane, Queensland

Queensland University of Technology, Brisbane, Queensland

Translational Research Institute, Brisbane, Queensland

University of Adelaide, Adelaide, South Australia

University of Technology, Sydney, New South Wales

Canada

AirBoss Defense, Acton Vale, Quebec

Canadian Border Services Agency, Ottawa, Ontario

Defence Research and Development Canada, Valcartier, Quebec

Ottawa Fire Services, Ottawa, Ontario

Public Health Agency of Canada, Winnipeg, Manitoba

Royal Canadian Mounted Police, Ottawa, Ontario

The SecDev Group, Ottawa, Ontario

Toronto Police Service, Toronto, Ontario

Transport Canada, Ottawa, Ontario

Uncharted Software, Inc., Toronto, Ontario

Ireland

D4H Technologies, Dublin

Israel

CONTROP Precision Technologies, Ltd., Hod Hasharon

Elbit Systems, Ltd., Yokneam

GenoSmart, Ltd., Reut

Israel Defense Forces

Israel Institute for Biological Research, Ness Ziona

Israel Ministry of Defense, Tel Aviv

Israel Police, Jerusalem

Israel Security Agency, Tel Aviv

Nuclear Research Center, Negev

Roboteam, Ltd., Tel Aviv

Sky Sapience, Ltd., Yokneam

Tamar Explosives, Ltd., Tel Aviv

Technion – Israel Institute of Technology, Tel Aviv

UVision Air, Ltd., Zur Igal

New Zealand

ikeGPS, Ltd., Wellington

Singapore

Defence Science and Technology Agency

Future Science and Technology Directorate

Ministry of Home Affairs

South Africa

SensePost Pty. Ltd., Pretoria

United Kingdom

Centre for the Protection of National Infrastructure

Cobalt Light Systems, Ltd., Abingdon

Defence Science and Technology Laboratory, Fort Halstead

Defence Science and Technology Laboratory, Porton Down

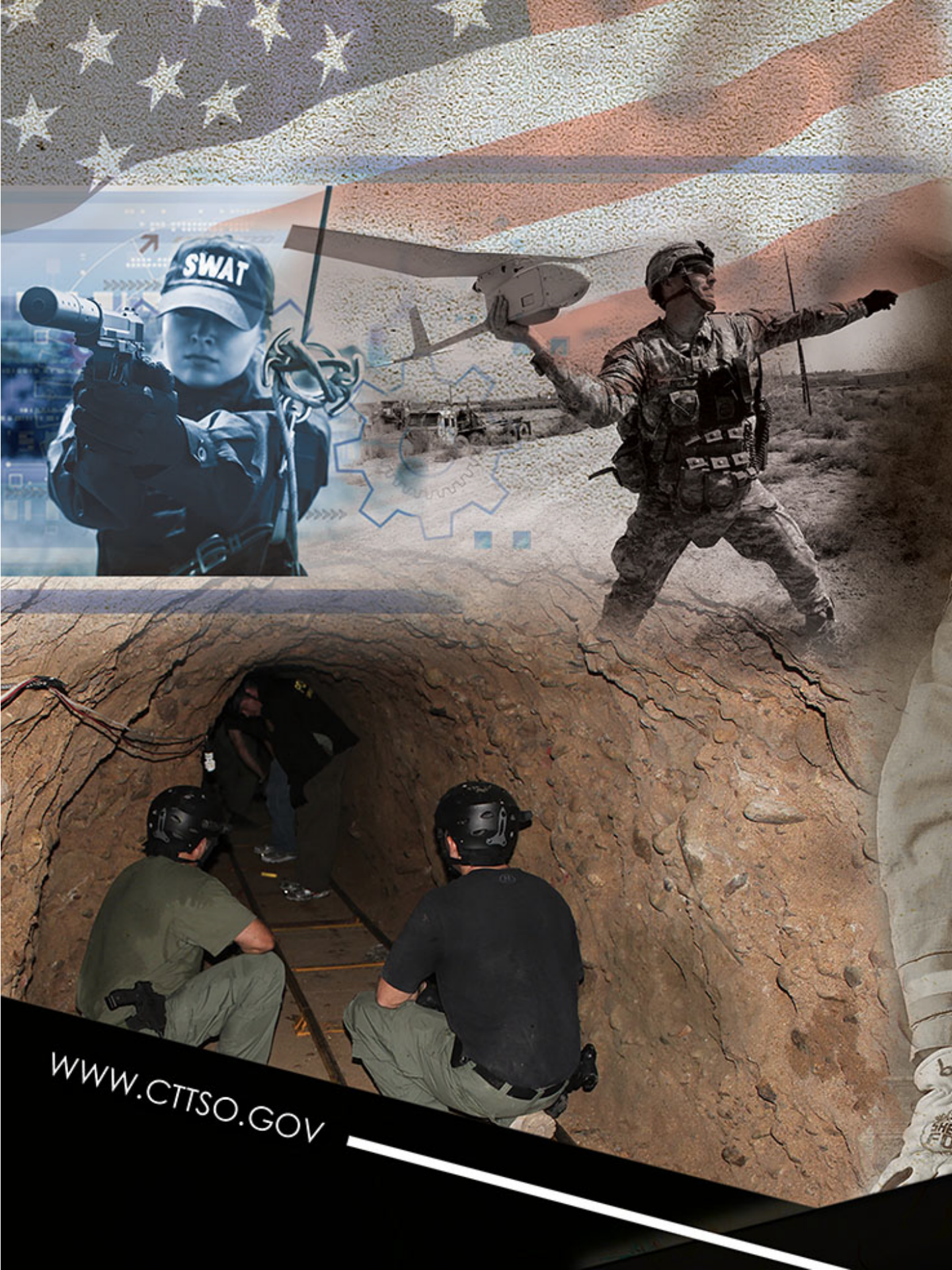
Defence Science and Technology Laboratory, Portsdown West

Landguard Systems, Ltd., Fareham

Intelligence Management Support Services, Ltd., Southampton

Ministry of Defence, London

New Century Consulting, London


SWAT
WWW.CTTSO.GOV